ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ТА КВАНТОВІ КОМП'ЮТЕРИ

Сьогодні Google повідомляє, що будь-який користувач може вилучити свої конфіденційні дані з результатів видачі їх пошуковиком Google. В "Android-асистент" тепер є розділ "Results about you". У ньому представлена інформація про власника смартфона, яка доступна іншим користувачам глобальної мережі.

Фахівці з кібербезпеки опублікували інструкцію з видалення з результатів видачі особистих даних, таких як номер телефону, домашня адреса, електронна пошта, персональні дані, номери карт і інше. Для видалення інформації про себе необхідно буде вказати причину цього кроку. Слід мати у виді, що персональні дані будуть вилучені Google тільки з результатів видачі. На сайтах, які виступають у ролі джерел інформації, вони залишаться.

Щоб захистити свої дані, технічні експерти рекомендують установити двофакторну аутентифікацію. Це подвійний захист, де перший рівень – це унікальні логін і пароль, а другий – доступ через СМС-паролі, пошту або додатки-аутентифікатори. Наприклад: ви вводите логін і пароль від Інтернет-банку, після на телефон приходить код по СМС або усередині додатка.

Разом з цим, згідно з повідомленням Daily Mail (масова британська щоденна газета), яка цитує експертів з кібербезпеки, майбутні квантові комп'ютери, які розробляються галузевими гігантами, такими як Google і IBM, зможуть зламувати шифрування, що захищає особисті дані, і розкривати особисту інформацію, включаючи банківські реквізити.

Шифрування з відкритим ключем – це метод, який використовується сучасними комп'ютерами для захисту даних, таких як приватне листування. Відкритий ключ будь-якого комп'ютера використовується пристроєм, який зв'язується з ним та шифрує його в довге число. Потім за допомогою свого закритого ключа пристрій використовує повідомлення для розшифровки.

Звичайним комп'ютерам потрібно приблизно 300 трильйонів років, щоб розшифрувати код, тому ця система, яка використовується з 1970-х років, досі цілком надійна. Однак це стане можливим із квантовими комп'ютерами. Вони зможуть розшифровувати дані з мільярдами шифрів за лічені секунди завдяки своїй величезній обчислювальній потужності, що дозволить вирішувати проблеми, на вирішення яких у сучасних комп'ютерів йдуть роки.

Обчислення будь-якого комп'ютера засновані на двійковому коді, але якщо в класичному комп'ютері біти або нулі, або одиниці, то в квантовому комп'ютері є кубіти, які можуть бути або нулями, або одиницями, або тим, і іншим одночасно.

"Квантовий апокаліпсис", відомий як Q-Day, – це назва ситуації, яка дана експертами з кібербезпеки, коли будь-хто, хто має потужний комп'ютер, може отримати доступ до зашифрованих даних. Уряди знають про цю можливість. Адміністрація Президента США Джо Байдена вже оголосила про плани оновити свою систему безпеки для захисту від квантової атаки до 2024 року. Корпорація IBM наприкінці минулого року представила машину Osprey, квантовий комп'ютер із рекордною обчислювальною потужністю.

Квантові біти, або кубіти, є мірою потужності квантового комп'ютера. Щодо класичних бітів (одиниць і нулів) у Всесвіті більше, ніж атомів, достатньо, щоб візуалізувати таку силу. Однак, як встановили дослідження китайських учених, комп'ютер не обов'язково має бути надзвичайно потужним, щоб розшифрувати надійне шифрування – достатньо показника із 378 кубітами. Поширення таких комп'ютерів прогнозується десь через 8 років.

Існуюча криптографія зрештою застаріє. Тому компанії намагаються створити "квантово-захищене" шифрування, стійке до потужностей квантових комп'ютерів.

Джерело: URL: https://cursorinfo.co.il/hi-tech/razrabotchiki-google-pridumali-kak-udalit-lichnye-dannye-iz-interneta
URL: https://t4.com.ua/tech/eksperty-poperedzhayut-pro-kvantovyj-apokalipsys-u-najblyzhchi-kilka-rokiv

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~