

В розрізі «Квантового повороту»: прогнози у галузі кібербезпеки

Що таке квантовий поворот?
Це «розум і соціальне життя. Це макроскопічні квантово-механічні явища», які впливають на наше життя. Це зрушення у нашому підході до всіх процесів які нас оточують. Класична суспільна наука, досі залишається домінуючою і заснована на вивченні реальних матеріальних об'єктів і сил, але суспільство навряд чи реальне чи відчутне. Ви можете торкатися тільки його локальних екземплярів, але не всієї чи абстрактної ідеї цього. Квантова фізика дає більш повне уявлення про реальність, тому що вона описує всі можливості всередині системи, які колапсують (декогерують) у класичному результаті у моменті виміру. Це не означає, що класична наука застаріла, це просто новий більш широкий погляд.

Кіберзлочинність обходиться економіці США у 100 мільярдів доларів на рік, а світовій економіці 450 мільярдів доларів.

Фхівці компанії Quantum Xchange, що займається забезпеченням «квантово-стійкої» кібербезпеки, опублікували у корпоративному блозі п'ятірку стислих галузевих прогнозів, пов'язаних з розвитком квантових комп'ютерів. Ось що, на думку експертів, набуває цього року надзвичайної актуальності на тлі стрімкого наближення «квантового повороту».

1. Підготовка до «Великої Міграції» (переведення систем безпеки в режим, що враховує існування квантових комп'ютерів) почнеться прямо зараз.

За кілька місяців свою підбірку

криптографічних протоколів, запропонованих як «постквантових», опублікує Національний інститут стандартів і технологій США (NIST). Вони, певне, стануть основою розробки нових стандартів. Після цього розпочнеться найбільша криптоміграція в історії обчислювальної техніки, яка триватиме кілька років та охопить усі організаційні рівні забезпечення безпеки.

2. Якщо підприємства не діятимуть, ігноруючи близькість «квантового повороту», це може мати для них негативні наслідки з боку страхування, а також з боку галузевих регуляторів. Власне страховики вже очікують від взаємодії поширених сьогодні протоколів безпеки з квантовими комп'ютерами (і зі штучним інтелектом, що стрімко розвивається) всього найгіршого, у зв'язку з чим підвищують тарифи. В останні роки вартість кіберстрахування стрімко зростає, а в третьому кварталі 2021 року в США (одна з двох країн, де найближчим часом, мабуть, розташовуватиметься більшість підприємств, що вкладають значні кошти в квантові обчислення), зросла на цілих 96%.

3. Головною метою атак будуть провайдери послуг комплексного управління IT-інфраструктурою, так звані MSP.

У нас є перед очима знаменитий приклад атаки хакерів на SolarWinds, саме такого провайдера, який управляє IT-структурами десятків тисяч приватних, корпоративних та державних користувачів. Зламавши продукт SolarWinds, зловмисники отримали у 2020 році адміністративний доступ до інформаційних мереж щонайменше 18

тисяч користувачів, серед яких кілька міністерств США та Великої Британії, британський Центр урядового зв'язку, Європарламент, компанія AstraZeneca etc. Логічно припустити, що сили, готові витратитися задля злему на квантові обчислення, з високою ймовірністю будуть бити якраз за структурами, що дозволяють, знайшовши одне слабке місце, отримати безліч інструментів впливу та збагачення. Очевидно, що саме таким провайдерам доведеться одними з перших розпочинати підготовку до «Великої міграції». Багатьом відповідальним користувачам водночас доведеться відмовитися від послуг MSP на користь індивідуальних рішень із власним контролем безпеки у кожній ланці кожного виробничого ланцюжка.

4. Зловмисники проникатимуть у мережі підприємств через домашні мережі співробітників.

Більшість експертів сходяться на тому, що віддалені робочі місця та гнучкі підходи до формування робочого простору масово збережуться і коли пандемія коронавірусної інфекції відступить. Тим часом, домашні мережі - це буквально відчинені ворота для хакерів, тому що в них зазвичай набагато більше вразливостей, ніж в професійно захищених корпоративних IT-середовищах. У світлі наближення квантового повороту бізнесам доведеться продумати додаткові заходи безпеки всього, що передається за межі підприємства і на кордон мережі (network's edge).

5. Продовжить набирати обертів

Джерело: <https://blogssmartzone.com>

американо-китайські перегони за квантове лідерство, що вже зараз нагадує змагання СРСР і США на зорі космічної ери за лідерство в космосі.

І хоча США більшою мірою зосереджують зусилля на розробці комерційного квантового комп'ютера, а Китай вкладається в основному в квантові комунікації, ця гонка все одно надаватиме потужний вплив на державний і приватний сектори по всьому світу, а насамперед — у самих США та Китаї. Причому вплив не завжди передбачуваний. Так інтерес Китаю до космічного квантового зв'язку підштовхнув Національне розвідувальне управління США (NRO) обмежити коло постачальників, що закуповуються управлінням з розвідувальними та геоінформаційними цілями комерційних зображень компаніями, що належать американцям, керованими американцями та контрольованими американцями. Тепер зображення не купуються навіть у підприємств, що базуються в союзних США країнах та схвалені як постачальники озброєння для американських збройних сил. Пентагон і Національне агентство геопросторової розвідки (NGA) — незадоволені, співробітники адміністрації Конгресу — спантеличені такою інтерпретацією NRO питань національної безпеки. Однак, мабуть, це не останній дивний побічний ефект боротьби двох найбільших економік світу за верховенство квантового майбутнього.

A

Підготував Геннадій Андрощук