УДК 004.056.55 **DOI:10.30837/rt.2022.2.209.01**

М.В. ЄСІНА, канд. техн. наук, О.В. ПОТІЙ, д-р техн. наук,
Ю.І. ГОРБЕНКО, канд. техн. наук, В.А. ПОНОМАР, канд. техн. наук

МЕТОДОЛОГІЯ ОЦІНКИ РИЗИКУ В ПОСТКВАНТОВИЙ ПЕРІОД

Вступ

У світі відбувається процес інтенсивного створення та застосування квантових технологій. Президент США підписав 4 травня 2022 р. «Меморандум про національну безпеку з просування лідерства в галузі квантових обчислень при одночасному зниженні ризиків для вразливих криптографічних систем, що свідчить про надзвичайну важливість квантових обчислень та їх застосування в криптології» [1]. Тому, просування лідерства в галузі квантових обчислень взагалі при одночасному зниженні ризиків для вразливих криптографічних систем є важливою проблемою. Відповідно на міжнародному та національному рівнях повинне бути обґрунтовано, прийняте та застосовуватись стандартизоване науково-методичне забезпечення оцінки ризиків взагалі для квантових обчислень, що є надзвичайно важливим для квантових обчислень при його застосуванні в криптології [1].

Метою цієї статі є обґрунтування та розробка методології оцінки ризиків для квантових обчислень при його застосуванні в криптології у так званий «постквантовий період» з урахуванням таких складових вирішення цієї проблеми [1 – 4]:

- використання способів боротьби із загрозами кібербезпеці, яка ще не виникла;
- визначення сутності методології квантової оцінки ризику;
- ідентифікація та документування інформаційних активів та їх поточний криптографічний захист;
- дослідження стану квантових комп'ютерів та квантово-безпечної криптографії. Оцінка термінів доступності цих технологій. Вплив на розробку та перевірку квантово-безпечної криптографії;
- визначення суб'єктів загрози та оцінка їх часу, необхідного для отримання доступу до квантової технології «z» [2];
- визначення часу існування ваших активів «x» і час, необхідний для перетворення технічної інфраструктури організації в квантово-безпечний стан «y» [2];
- визначення квантового ризику за допомогою обчислення, чи стануть бізнес-активи вразливими, перш ніж організація зможе їх захистити;
- визначення та розставлення пріоритетів заходів, необхідних для підтримки обізнаності та переведення технологій організації в квантово-безпечний стан;
- визначення та застосування варіантів захисту від квантових загроз на даний момент.

1. Можливості реалізації квантових обчислень, переваги та недоліки

1.1. Класифікація перспективних фізичних реалізацій квантових комп’ютерів

На основі робіт [2 – 5] створена високорівнева класифікація перспективних фізичних реалізацій квантових комп’ютерів:

• Квантова оптика, коли інформація зберігається та захищається в станах квантів світла на основі поляризації або станах з певним числом фотонів, та може бути реалізована в чіпі за допомогою інтегрованої оптики.

• Надпровідні системи, коли інформація зберігається та обробляється (захищається) в електричних ланцюгах, які використовують властивості надпровідних матеріалів.

• Топологічні системи, коли інформація зберігається та захищається з використанням деяких топологічних властивостей, тобто властивостей, які залежать від «глобальних» (геометричних) властивостей, нечутливих до «локальних» змін – квантових систем.

• Іонні пастки, коли інформація зберігається (захищається) та маніпулюється з використанням властивостей іонів (атомів із незникаючим повним електричним зарядом), які обмежені електромагнітними полями.

• Квантові спінові системи, коли інформація зберігається (захищається) та маніпулюється у внутрішньому ступені свободи, який називається квантовим спіном. Такі системи можуть бути реалізовані в кремнії, як стандартні мікрочіпи, або в менш звичайних системах, як алмази з точковими дефектами, відомі як азотно-заміщена (коротше NV) вакансія [5].

Гази холодних атомів, де нейтральні атоми (а не іони) охолоджуються до значення близького до абсолютного нуля. У той час як іони відштовхуються один від одного через свій електричний заряд, нейтральні атоми цього не роблять, і можуть бути захоплені і організовані в дуже регулярні масиви за допомогою лазерних променів, що створюють так звані оптичні решітки. Атомами можна керувати аж до рівня окремих ділянок в решітці.

1.2. Основні переваги та недоліки квантових комп'ютерів

Основними перевагами та недоліками фізичних реалізацій квантових комп'ютерів є [1, 5]:

• масштабованість, тобто можливість створення та управління все більшими і більшими квантовими пристроями зі все більшою кількістю кубітів, використовуючи фізичні/інженерні ресурси, які керуються керованим способом;

• сумісність з різними обчислювальними моделями та простота їх реалізації;

• типовий час декогерентності (тобто скільки часу залишаються збереженими характеристики та використані в працездатному стані, а також можуть бути використані квантові особливості, такі як суперпозиції);

• швидкість і точність, з якою вентилі можуть бути застосовані.

1.3. Стан розроблення та прийняття в якості національного постквантових стандартів в Україні

Основним застосуванням квантових обчислень є забезпечення криптографічної стійкості певних криптографічних властивостей від класичних та квантових атак, атак на основі помилок та спеціальних атак [7].

Наразі в Україні в якості національного стандарту прийнято постквантовий стандарт криптографічних перетворень асиметричного шифрування та інкапсуляції ключів ДСТУ 8961-2019, розроблено та знаходяться на етапі прийняття проєкти національних стандартів електронного підпису (ЕП) «Вершина» та «Сокіл». Держспецзв'язку, ТК-20 та Національний центр стандартизації проводять роботу з прийняття в якості національного постквантового проєкту стандарту ЕП «Вершина» та проводять громадське обговорення щодо прийняття рішення відносно проєкту постквантового національного стандарту ЕП «Сокіл». Прийняті та впроваджуються національні постквантові стандарти симетричних криптоперетворень ДСТУ 7624-2014, ДСТУ 7564-2014 та ДСТУ 8845-2019. Наука, що стоїть за квантовими комп'ютерами, бере свій початок з фізики квантової механіки, яка вносить фундаментальні зміни в наше розуміння Всесвіту. Багато фізиків мали проблеми з цими революційними ідеями, але експерименти та спостереження підтвердили квантову теорію, і її основні принципи очевидні в звичайних пристроях, таких як лазери та транзистори. Ці технології лише натякають на повну перспективність квантової техніки, але ще потрібна значна робота, перш, ніж буде можливість створити справжній квантовий комп'ютер [1 – 7].

1.4. Стан розроблення та використання квантових комп'ютерів у світі

Коли ефективні квантові комп'ютери [1 – 7] стануть доступними, вони по суті усунуть криптографічну складність існуючих криптосистем з відкритим ключем. Більш традиційні криптосистеми із спільним ключем (такі як AES) також будуть уразливими, що знизить їх ефективну надійність безпеки приблизно до половини того, що є на сьогоднішній день. Цей факт матиме руйнівний вплив на системи, що використовуються для захисту електронних комунікацій та цифрових транзакцій. Більшість безпечних Інтернет-процесів орієнтується на протоколи, які використовують криптографію з відкритим ключем, включаючи ті, що використовуються для захисту веб-сайтів, банківських транзакцій, безпечної електронної пошти та електронних підписів.

Квантові комп'ютери використовують обчислювальну потужність квантових систем і дають можливість вирішувати обчислювальні проблеми, які раніше вважалися важкорозв'язними. Квантові особливості, на які покладаються квантові комп'ютери, дуже важко зберегти та контролювати. Саме це робить створення квантового комп'ютера складним завданням. Однак, будучи створеними, квантові комп'ютери зламають деякі основи інфраструктури кібербезпеки.

Квантову загрозу кібербезпеці можна пом'якшити шляхом розгортання нових криптографічних інструментів (як звичайних, так і квантових), які, як вважається та/або відомо, є стійкими до квантових атак. Тим не менш, перехід до квантово-безпечної криптографії сам по собі є проблемою, оскільки вимагає розробки та розгортання апаратних і програмних рішень, встановлення стандартів, міграції застарілих систем тощо.

Стан розроблення та застосування квантових комп'ютерів для криптоаналізу наведено нижче [6]:

- IBM повідомила про план запуску в жовтні 2019 р. 53-кубітного квантового комп'ютера (КВК);
- 53-кубітний КВК IBM має нову конструкцію процесора, має можливість масштабуватись, знижена ймовірність помилок, надійний в хмарі;
- IBM відкриває новий обчислювальний центр в Нью-Йорку, 1–53 кубіт, 5–20 кубіт (14 в перспективі);
- 72-кубітний КВК Google за 3,5 хвилини виконує еквівалент роботи 10 тисяч операцій надпотужного кластера.

Згідно з [9, 11] IBM представили квантовий 127-кубітний процесор Eagle. Він прийшов на зміну 65-кубітному квантовому процесору Hummingbird, що відповідає дорожній карті квантових технологій від IBM [10]. Як зазначено в [9], відмінністю Eagle від попередніх процесорів полягає в тому, що він потребує значно меншої кількості електроніки для контролю та зчитування на кубіт регістру завдяки застосуванню мультиплексування зчитування. Також IBM повідомляють про наміри щодо побудови нової інтегрованої квантової обчислювальної системи IBM Quantum System Two на основі покращених чіпів, замість вже існуючої системи IBM Quantum System One.

Також є відомості [11] про наміри IBM представити 433-кубітний процесор Osprey наступного року, та 1121-кубітного процесору Condor в 2023 році, що відповідає дорожній карті, наведеній в [10].

В той самий час, компанія D-wave, що відома своїми розробками в сфері побудови псевдо-квантових (гібридних) комп'ютерів з великою загальною кількістю кубітів (понад 2000 кубітів на початку та понад 5000 кубітів сьогодні), повідомила про наміри представити машину із загальною кількістю кубітів понад 7000 близько 2023 – 2024 року та про наміри щодо розробки власних надпровідникових квантових машин гейтового типу (розробкою яких наразі замаються IBM, Google та інші) [12].

Зрозуміло, що фактичний стан розроблення та застосування квантових комп'ютерів та їх математичного та програмного забезпечення є строго конфіденційним та надійно захищається.

Сутність та стан вирішення проблеми постквантової криптографії на світовому рівні – NIST США провів три етапи конкуру щодо кандидатів на стандарти постквантових асиметричних криптографічних примітивів. Наразі проведено семінар, на якому розглянуто попередні підсумки 3-го етапу конкурсу проєктів асиметричних криптографічних перетворень.

Основні вимоги до кандидатів на стандарти постквантових криптоперетворень можна конкретизувати у трьох напрямках [7, 8]:

- вимоги з безпеки (вимоги щодо стійкості до криптографічного аналізу);
- техніко-економічні вимоги (в основному щодо часової та просторової складностей);
- технічні характеристики реалізації алгоритмів асиметричних криптоперетворень.

Вимоги до стійкості ЕП мають бути сформульовані у відповідності до моделі загроз EUF-CMA (Existentially unforgeable under adaptive chosen message attacks), тобто забезпечення захисту від екзістенційної підробки при атаках на основі адаптивно підібраного (вибраного) шифртексту [8].

1.5. Вимоги до параметрів квантових комп'ютерів

Основними вимогами є:

- час міграції: кількість років для міграції системи до квантово-безпечного рішення;
- часова шкала загроз: кількість років до того, як відповідні суб'єкти загрози зможуть зламати квантово-вразливі системи.

Якщо термін загрози менший за суму терміну зберігання та часу міграції, організації не зможуть захистити свої активи протягом необхідних років від квантових атак. Краще розуміння часової шкали загроз надає інформацію про час, доступний для безпечного переходу до постквантових кіберсистем.

Оцінити квантові загрози дуже складно через наукові та інженерні перешкоди, пов'язані з побудовою працюючого квантового комп'ютера. Експерти загалом визнають, що досі не знають, коли з'являться квантові комп'ютери, які можуть загрожувати кіберсистемам. Проте було б дуже корисно мати уявлення про перспективи цієї загрози, що стане реальною в короткостроковій та середньостроковій перспективі, про швидкість прогресу та про основні віхи, на які слід звернути увагу менеджерам із кіберризиків.

Основною проблемою в побудові квантового комп'ютера є створення надійних фундаментальних компонентів, так званих фізичних кубітів, кількість яких можна масштабувати, зберігаючи контроль і якість. У цьому відношенні експерти вказали, що найбільш перспективною фізичною платформою для реалізації криптографічно релевантного квантового комп'ютера є надпровідні системи, за якими відносно близько слідують захоплені іони, а також кілька інших фізичних реалізацій, що мають значний потенціал.

Дуже важливим кроком вперед буде експериментальна демонстрація того, що схеми виправлення помилок покращують надійність так званих логічних кубітів у порівнянні з фізичними кубітами. Щоб це сталося, має бути можливість достатньо добре підготувати, маніпулювати та виміряти основні фізичні кубіти. Наскільки добре має бути це «досить добре», залежить від найвідоміших схем виправлення помилок, які самі по собі можуть бути замінені новими та кращими схемами.

Іншим етапом стане демонстрація так званої «квантової переваги», тобто здатності квантового пристрою виконувати певні обчислення, які були б практично неможливими навіть для найпотужнішого класичного суперкомп'ютера, незалежно від корисності таких обчислень. Хоча досягнення квантової переваги не обов'язково призведе до вирішального криптографічного прогресу стосовно квантового комп'ютера, це означатиме досягнення відносно високого рівня контролю над відносно великою кількістю фізичних кубітів, що є

необхідною складовою для квантових обчислень. Експерти погодилися, що цей етап, ймовірно, буде пройдено в найближчі пару років [5].

2. Методологія оцінки ризику в постквантовий період

2.1. Способи боротьби із загрозою, яка ще не виникла

Незважаючи на постійний прогрес у розвитку квантових обчислень, ймовірно, що реально квантові комп'ютери стануть доступними та будуть застосовуватись для криптоаналізу, щонайменше через 5 – 15 років [2 – 8]. Можливо, це пояснює низький рівень занепокоєння тих, хто відповідає за планування кібербезпеки та прийняття рішень. Безсумнівно, їхня увага зосереджена на безлічі кіберзагроз, з якими сьогодні стикаються всі організації, і, можливо, вони вважають, що буде достатньо часу, щоб відповісти, як тільки квантові комп'ютери справді з'являться.

Щодо цієї точки зору є декілька проблем. Як тільки квантовий комп'ютер буде винайдено, це негайно вплине на безпеку всіх Інтернет-комунікацій і даних. Якщо організації не будуть готові до цієї раптової кризи, вони зіткнуться з негайною потребою замінити свої існуючі криптографічні системи безпеки на квантово-безпечні рішення.

Адаптація всієї криптографічної інфраструктури організації в період, коли всі інші намагаються зробити те ж саме, ймовірно, буде складною і дорогою. Небагато організацій самостійно розробляють можливості криптографічної безпеки, більшість отримує їх у постачальників, часто інтегрованих у мережу чи продукти безпеки. Без попередньої підготовки організація може не мати уявлення про здатність своїх постачальників надавати квантово-безпечні рішення, а також не знати про труднощі, з якими вона зіткнеться при інтеграції нової технології в своє середовище. Однак це не єдина проблема, з якою можуть зіткнутися погано підготовлені організації.

Було запропоновано кілька квантово-безпечних рішень, але небагато з них вийшли з фази дослідження, і навіть вони потребують багато роботи, щоб перевірити, чи можуть вони протистояти як звичайним, так і квантовим атакам. Протягом останніх 15 або більше років поточні протоколи кібербезпеки стикалися з реальними проблемами та перейшли до свого поточного стану. Ми довіряємо їм частково через їх математичні основи, а також тому, що вони витримали випробування часом. Якщо ми хочемо довіряти квантово-безпечній криптографії, важливо, щоб тестування в реальному світі розпочалося якомога швидше.

Управління цією проблемою вимагатиме усвідомлення, планування та підготовки. Добре підготовлена організація може вжити заходів для інтеграції квантово-безпечних рішень у існуюче планування кібербезпеки та управління життєвим циклом, де їх можна оцінити на предмет функціональності, продуктивності, простоти використання та інших факторів. При необхідності існуючу інфраструктуру можна покращити або замінити. І все це може статися до того, як ці зміни стануть критичними для безпеки організації.

Організації також повинні мати можливість захищати свою конфіденційну інформацію протягом усього терміну її існування. Інформація, яка вважається безпечною для зберігання або передачі, оскільки вона зашифрована, може стати вразливою для квантового комп'ютера протягом його життя. Розуміння цього ризику вимагає вивчення поточних засобів кіберзахисту та доступу суб'єктів потенційної загрози до технології квантових обчислень.

Управління переходом повного набору інструментів, що використовуються для захисту різноманітних бізнес-функцій та інформаційних активів, може здатися складним завданням без чіткої відправної точки чи пріоритетів.

Квантова оцінка ризику – це ідеальний підхід для виявлення та визначення пріоритетів загроз і вразливостей, а також закладання основи для надійного та економічно ефективного розвитку систем, щоб вони були стійкими до квантових атак.

2.2. Сутність методології квантової оцінки ризику

Квантова оцінка ризику дає організації знання, необхідні для розуміння ступеня їх квантового кіберризику та термінів, за які можуть виникнути квантові загрози. Це забезпечить організацію основою для проактивного вирішення квантових ризиків, побудови шляху до квантово безпечного стану, а також для впровадження та підтвердження квантово-безпечних рішень як частини нормального управління життєвим циклом, а не як відповідь на кризу.

Квантова оцінка ризику (QRA) не замінює звичайну оцінку кіберризику (RA). Частина інформації, зібраної під час RA, також вимагається квантовим процесом, тому QRA зазвичай проводиться разом із традиційним RA або після нього. Однак QRA зосереджена на конкретних питаннях безпеки, які виникають у квантових комп'ютерах; вона не стосується безпосередньо кількох аспектів традиційного процесу оцінювання.

Кілька років тому Mosca запропонував модель для оцінки квантового ризику [2]. Описаний далі шестифазний процес QRA узгоджується з моделями оцінки ризиків таких організацій, як NIST, а також включає квантову модель ризику Mosca «x, y, z».

2.2.1. Фаза 1 «Ідентифікація та задокументування інформаційних активів та їх поточний криптографічний захист»

Як і будь-яка оцінка ризику, QRA починається з інвентаризації важливих активів. У центрі уваги тут є чутливі або цінні інформаційні активи, які потребують криптографічного захисту відповідно до політики безпеки організації. Важливо визначити характер використовуваної криптографії, спосіб створення, зберігання та застосування ключів шифрування, а також походження інструментів або пристроїв, які використовуються в цих процесах.

На високому рівні організація повинна розуміти природу своєї конфіденційної/цінної інформації, включаючи її цінність для бізнесу, механізми контролю доступу та спільного використання даних, процедури резервного копіювання та відновлення, а також те, як вона обробляється наприкінці терміну служби. Багато організацій мають правові або нормативні вимоги, які впливають на це. Для визначення вразливості організації до зовнішніх і внутрішніх загроз необхідний комплексний огляд усіх цих факторів.

2.2.2. Фаза 2 «Дослідження стану квантових комп'ютерів та квантово-безпечної криптографії. Оцінка термінів доступності цих технологій. Вплив на розробку та перевірку квантово-безпечної криптографії»

Ця фаза не є унікальною для конкретної QRA, це скоріше безперервний процес, який проводиться групою експертів з квантових технологій, які розуміють перешкоди та події, з якими стикаються в кількох галузях квантових досліджень, і можуть використовувати інформацію для прогнозування ймовірних термінів для надання квантового комп'ютера та розуміння його впливу на кібербезпеку організації.

Існує багато джерел інформації про стан квантових технологій, але розуміння актуальності та справжнього впливу конкретних дослідницьких розробок не є тривіальним процесом. Наявність спеціальної команди експертів з квантової галузі або відносини з організацією, що спеціалізується на квантових технологіях, є надзвичайно важливим для завершення QRA. У всьому світі існує кілька груп, які проводять незалежні дослідження та використовують різні підходи до розробки квантових комп'ютерів і квантово-безпечної криптографії. Важливо мати доступ до експертів, які стежать за подіями в обох сферах і можуть контекстуалізувати їх, щоб прогнозувати їхній вплив на кібербезпеку.

В ідеалі результати цієї фази QRA використовуються для впливу на розвиток квантово-безпечної криптографії. Робота з квантовими експертами, які мають міцні зв'язки з академічними та дослідницькими спільнотами, дозволяє реальним проблемам, виявленим QRA, впливати на напрямок квантово-безпечних досліджень.

2.2.3. Фаза 3 «Визначення суб'єктів загрози та оцінка їх часу, необхідного, щоб отримати доступ до квантової технології «z»»

Організація, яка піклується про безпеку, знатиме всі загрози для своїх найбільш значущих суб'єктів та матиме список попередніх спроб проникнути в їхній кіберзахист. QRA розглядає вплив квантових обчислень на ці загрози, зосереджуючи увагу на ймовірності того, що вони зможуть використовувати квантові комп'ютери, і часові межі доступу до них. Також треба розглядати нові діючі сторони загроз, які можуть з'явитися, коли квантові обчислення стануть реальністю. У сукупності вони утворюють частину Collapse Time (z) моделі Mosca, тобто час, доки поточні засоби кіберзахисту не впадуть перед загрозами, які мають доступ до квантових технологій.

Цей процес знову вимагає постійної оцінки експертів, які знають розвиток кібербезпеки та квантових обчислень.

2.2.4. Фаза 4 «Визначення часу існування ваших активів «x» і час, необхідний для перетворення технічної інфраструктури організації в квантово-безпечний стан «y»»

Визначення терміну служби бізнес-інформації має вирішальне значення для розуміння квантової вразливості організації. Якщо зловмисник може захопити та заархівувати зашифровану інформацію, як довго вона буде корисною? Це регулюватиметься характером бізнесу, продуктів і клієнтів, а також нормативними вимогами, які можуть застосовуватися до організації.

Розглядаються доступні інструменти для боротьби з квантовими загрозами. Наскільки ефективні поточна політика та процедури щодо захисту зашифрованої інформації організації як від внутрішніх, так і від зовнішніх загроз? Досліджується міцність існуючої криптографії та наскільки ефективно вона застосовується та використовується. Розглядаються доступні квантово-безпечні криптографічні методи, щоб визначити, чи можуть вони бути доречною заміною існуючих можливостей. Можна зв'язатися з постачальниками, які виготовили продукти, які використовуються в організації, щоб визначити, чи можна впровадити нові алгоритми або протоколи в існуючі інструменти та пристрої, чи може знадобитися оновлене обладнання. Переглядаючи політику, процеси управління та закупівлі, які застосовуються до IT та інфраструктури безпеки організації, оцінюється, чи можна інтегрувати квантову безпеку в процеси управління життєвим циклом IT організації.

Маючи цю інформацію, можна обчислити решту значень моделі Mosca – термін зберігання даних організації (x) та час міграції інфраструктури (y).

2.2.5. Фаза 5 «Визначення квантового ризику за допомогою обчислення, чи стануть бізнес-активи вразливими, перш, ніж організація зможе їх захистити (x+y>z?)»

Використовуючи інформацію, зібрану до цього моменту, можна оцінити ризик, з яким стикається організація, коли з'являються квантові комп'ютери. Враховується тривалість життя конфіденційних даних, включаючи ймовірність їхнього впливу. Це порівнюється з проміжком часу, протягом якого квантові технології будуть доступні відповідним суб'єктам загрози. У сукупності це дає розумну оцінку того, коли організації необхідно вжити активних заходів для пом'якшення квантового ризику. Цілком можливо, що деякі організації вже стикаються з цим ризиком, залежно від терміну життя їхніх даних і процесів, які діють для їх захисту сьогодні.

Далі необхідно оцінити вплив на бізнес-процеси, який є результатом очікуваних змін:

- скільки часу знадобиться для впровадження необхідних змін у продукти, протоколи та процедури?
- чи призведуть квантово-безпечні технології до проблем із затримками, надійністю чи продуктивністю, які потребують вирішення?
- чи потрібні зміни в політиці чи процедурі для покращення переглянутої системи чи загальної безпеки інформації організації?

2.2.6. Фаза 6. «Визначення та розставлення пріоритетів заходів, необхідних для підтримки обізнаності та переведення технологій організації в квантово-безпечний стан»

Квантова оцінка ризику надає інформацію та вказівки щодо статусу квантової безпеки, але навряд чи цього стану можна досягти за допомогою інструментів і технологій, доступних сьогодні. Квантові технології продовжують розвиватися, як і наше розуміння сильних і вразливих сторін квантово-безпечних підходів. Плани міграції також повинні реагувати на зміни, оскільки постачальники включають ці розробки у свої продукти та інструменти. Важливо відстежувати все це, і більшість організацій повинні розробити план, який вирішує безпосередні проблеми, дозволяючи впроваджувати нові квантові технології, коли вони стають доступними.

Будь-яку оцінку кіберризиків необхідно періодично оновлювати, щоб врахувати нові загрози та скористатися перевагами покращених рішень безпеки. Особливо це стосується квантових технологій, які швидко розвиваються. Зараз досліджуються різні варіанти квантових технологій, але не всі вони створюють однакову загрозу кібербезпеці, і може бути важко оцінити вплив будь-якої нової квантової розробки. Тому рекомендується, щоб QRA була першим кроком у створенні шляху до квантової безпеки.

Цей шлях буде розроблений для забезпечення постійного доступу до фахівців, які дотримуються цих технологій і розуміють наслідки нових розробок у квантових обчисленнях і квантовій криптографії. Це може стати основою для початку обговорення з працівниками організації, партнерами, клієнтами та постачальниками продуктів, гарантуючи, що всі знають про кроки, які вживаються, і переконавшись, що вони розуміють який вплив це матиме на їхні власні процеси та інфраструктуру.

Висновки

1. Квантова оцінка ризику – це ідеальний підхід для виявлення та визначення пріоритетів загроз і вразливостей, а також закладання основи для надійного та економічно ефективного розвитку систем, щоб вони були стійкими до квантових атак.

2. Квантова оцінка ризику дає організації знання, необхідні для розуміння ступеня їх квантового кіберризику та термінів, за які можуть виникнути квантові загрози. Це забезпечить організацію основою для проактивного вирішення квантових ризиків, побудови шляху до квантово безпечного стану, а також для впровадження та підтвердження квантово-безпечних рішень.

3. Квантова оцінка ризику (QRA) не замінює звичайну оцінку кіберризику (RA). Частина інформації, зібраної під час RA, також вимагається квантовим процесом, тому QRA зазвичай проводиться разом із традиційним RA або після нього.

4. У [2] Mosca запропонував модель для оцінки квантового ризику. Описаний шестифазний процес QRA узгоджується з моделями оцінки ризиків таких організацій, як NIST, а також включає квантову модель ризику Mosca «x, y, z».

5. Якщо організація використовує будь-яку інформаційну технологію, то криптографія завжди використовується для кібербезпеки. Тому не можна дозволити чекати появи квантових комп’ютерів, щоб зрозуміти ризики, з якими можна стикнутись.

6. Необхідно вжити наступні заходи для того щоб [2 – 8]:

• переконатися, що є наявним поточний, ретельний організаційний інвентар, який містить відомості про вбудовану криптографію, яка може існувати в різних продуктах;

• відстежувати оточення на предмет загроз і забезпечувати регулярну оцінку ризиків;

• проводити квантову оцінку ризику як частину регулярного процесу оцінки ризику або після нього;

• зрозуміти позицію постачальників телекомунікацій та безпеки щодо квантових обчислень, на які з їхніх продуктів це вплине, а також про те, як вони підготуються до управління цим ризиком;

• оцінити квантову готовність як частину ваших поточних процесів закупівлі мереж і систем безпеки, обговорити стан квантового планування поточних постачальників;

• співпрацювати з інформованим партнером, щоб відстежувати розвиток квантових обчислень і квантово-безпечних рішень, а також створити план квантової готовності для організації.

7. Найбільшому ризику піддаються організації, які чекають на прибуття квантових комп'ютерів або уникають дій, поки не будуть розроблені ідеальні криптографічні рішення. Це напевно змусить таку організацію боротися зі своєю раптовою вразливістю до квантової атаки в осяжному майбутньому.

Список літератури:

1. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. [Електронний ресурс]. Режим доступу: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.
2. Michele Mosca, John Mulholland A Methodology for Quantum Ass Risk Assessment. [Електронний ресурс]. Режим доступу: https://globalriskinstitute.org/publications/3423-2/.
3. Mosca M., Piani M. (2019). Quantum Threat Timeline. Global Risk Institute. [Електронний ресурс]. Режим доступу: https://globalriskinstitute.org/publications/quantum-threat-timeline/.
4. Mosca M., Piani M. Quantum Threat Timeline Report 2020. Global Risk Insitute. [Електронний ресурс]. Режим доступу: https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/.
5. Mosca M., Piani M. Quantum Thremtntat Timeline Report 2021. Global Risk Insitute. [Електронний ресурс]. Режим доступу: https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/.
6. Viktor Onoprienko The state of innovative research and development in the field of information security in Ukraine (JSC "IIT") / Viktor Onoprienko, Marina Yesina, Ivan Gorbenko, Yuri Gorbenko, Elena Kachko // Forum: Innovative solutions in a digitalized economy: Germany – Ukraine. [Електронний ресурс]. Режим доступу: https://www.facebook.com/events/596729504987733/.
7. Gorjan Alagic NISTIR 8309 Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process / Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone. Режим доступу: https://doi.org/10.6028/NIST.IR.8309.
8. Горбенко Ю. І. Побудування та аналіз систем, протоколів та засобів криптографічного захисту інформації / Ю. І. Горбенко, за ред. Горбенко І. Д. Харків : Форт, 2016. 959 с.
9. IBM Quantum breaks the 100-qubit processor barrier. IBM Research Blog. [Електронний ресурс]. Режим доступу: https://research.ibm.com/blog/127-qubit-quantum-processor-eagle.
10. IBM's roadmap for scaling quantum technology. IBM Research Blog. [Електронний ресурс]. Режим доступу: https://research.ibm.com/blog/ibm-quantum-roadmap.
11. First quantum computer to pack 100 qubits enters crowded race. Nature News. Philip Ball [Електронний ресурс]. Режим доступу: https://www.nature.com/articles/d41586-021-03476-5.
12. IBM claims advance in quantum computing. BBC News. Paul Rincon. [Електронний ресурс]. Режим доступу: https://www.bbc.com/news/science-environment-59320073.
13. D-Wave plans to build a gate-model quantum computer. TechCrunch. Frederic Lardinois. [Електронний ресурс]. Режим доступу: https://techcrunch.com/2021/10/05/d-wave-plans-to-build-a-gate-model-quantum-computer/.

Надійшла до редколегії 02.03.2022

Відомості про авторів:

Єсіна Марина Віталіївна – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; науковий співробітник-консультант АТ «ІІТ»; Україна; e-mail: rinayes20@gmail.com; ORCID: https://orcid.org/0000-0002-1252-7606

Потій Олександр Володимирович – д-р техн. наук., професор, полковник, заступник Голови Державної служби спеціального зв'язку та захисту інформації; Україна; e-mail: potav@ua.fm; ORCID: https://orcid.org/0000-0002-2366-0541

Горбенко Юрій Іванович – канд. техн. наук, АТ «Інститут інформаційних технологій», перший заступник головного конструктора; Україна; e-mail: gorbenkou@iit.kharkov.ua; ORCID: https://orcid.org/0000-0003-0073-9107

Пономар Володимир Андрійович – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, науковий співробітник кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: Laedaa@gmail.com; ORCID: https://orcid.org/0000-0001-5271-2251