МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

САРАПУК Олег Ігорович

Алгоритм побудови мереж квантового розподілу ключів / Algorithm for Building Quantum Key Distribution Networks

спеціальність: 125 – Кібербезпека та захист інформації

освітньо-професійна програма –Кібербезпека

Кваліфікаційна робота

Виконав студент групи КБм -21
О.І. Сарапук

Науковий керівник
д.т.н., професор М.М.Касянчук

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2025 р.

Завідувач кафедри
_____ В.В.Яцків

ТЕРНОПІЛЬ – 2025

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь "магістр"
спеціальність:125 – Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ В.В.Яцків
"____"_____2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
САРАПУКУ Олегу Ігоровичу

(прізвище, ім'я по-батькові)

1. Тема кваліфікаційної роботи
Алгоритм побудови мереж квантового розподілу ключів / Algorithm for Building Quantum Key Distribution Networks
керівник роботи: д.т.н., професор М.М.Касянчук
затверджені наказом по університету від 29 листопада 2024 року № 938
2. Строк подання студентом закінченої кваліфікаційної роботи
5 грудня 2025 р.
3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.
4. Основні питання, які потрібно розробити

– проаналізувати сучасні технології генерації ключів для криптографічних перетворень;

– розробити спосіб побудови класичного автентифікованого каналу квантової апаратури;

– визначити функції універсального хешування для формування міток автентифікації;

– розробити вимоги до структури мережі КРК, рівня споживачів та рівня генерації квантових ключів;

– розробити рекомендовану структуру мережі КРК та методику побудови мережі КРК змішаної топології.

5. Перелік графічного матеріалу у роботі.

Послідовність виконання протоколу КРК
Спосіб передавання секретного ключа «матрьошкою».
Схема диверсифікації квантових ключів протоколу КРК.
Структура мережі КРК (по рівнях).
Інтерфейси взаємодії між різними рівнями мережі.

Структура мережі КРК (по вузлах).
Блок-схема процесу розподілу КЗК.
Методика побудови мережі КРК.

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання: 29 листопада 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз особливостей генерації квантових ключів	12.2024 р. – 03.2025 р.	
2	Побудова автентифікованого каналу для квантової генерації ключів	03.2025 р. – 06.2025 р.	
3	Алгоритм побудови мережі КРК	06.2025 р. – 11.2025 р.	

Студент _____ Сарапук О.І.
(підпис)

Керівник роботи _____ д.т.н., проф. Касянчук М.М.
(підпис)

АНОТАЦІЯ

Сарапук О.І. Алгоритм побудови мереж квантового розподілу ключів. – Рукопис.

Дослідження на здобуття освітнього ступеня «магістр» за спеціальністю 125 «Кібербезпека та захист інформації», освітньо-професійна програма «Кібербезпека». – Західноукраїнський національний університет, Тернопіль, 2025.

Здійснено аналіз сучасних технологій генерації ключів для криптографічних перетворень та відомих способів подолання максимальної дальності під час створення квантових ключів. На основі аналіз структури мережі квантового розподілу ключів за версією ETSI розроблено алгоритм побудови автентифікованого каналу квантової апаратури та обгрунтовано варіанти використання хеш-функцій для автентифікації. Згідно встановлених вимог до рівнів споживачів, генерації квантових ключів та формування квантовозахищених ключів розроблено алгоритм побудови мережі квантового розпоілу ключів. Розроблено методику побудови та рекомендовану структуру мережі квантового розпоілу ключів.

Ключові слова: ШИФРУВАННЯ, МЕРЕЖА, КЛЮЧІ, КВАНТОВИЙ РОЗПОДІЛ, КРИПТОАЛГОРИТМИ, ПОЛЯРИЗАЦІЯ.

ABSTRACT

Sarapuk O.I. Algorithm for Building Quantum Key Distribution Networks. – Manuscript.

Research for the degree of "Master" in specialty 125 "Cybersecurity and information protection", educational and professional program "Cybersecurity". – West Ukrainian National University, Ternopil, 2025.

An analysis of modern technologies for generating keys for cryptographic transformations and known methods for overcoming the maximum range during the creation of quantum keys was carried out. Based on the analysis of the structure of the quantum key distribution network according to the ETSI version, an algorithm for constructing an authenticated channel of quantum equipment was developed and options for using hash functions for authentication were substantiated. According to the established requirements for consumer levels, quantum key generation and quantum-protected key formation, an algorithm for constructing a quantum key distribution network has been developed. A construction methodology and a recommended structure of a quantum key distribution network have been developed.

Keywords: ENCRYPTION, NETWORK, KEYS, QUANTUM DISTRIBUTION, CRYPTOALGORITHMS, POLARIZATION.

ЗМІСТ

ВСТУП

Сучасні інформаційні системи функціонують в умовах стрімкого зростання обсягів переданих даних і посилення кіберзагроз [1-3]. Класичні методи захисту, які грунтуються на обчислювальній складності математичних задач (факторизація великих чисел, обчислення дискретного логарифма тощо), перебувають під реальною загрозою через розвиток квантових обчислень [4, 5]. Уже зараз доведено, що алгоритм Шора здатний ефективно розв'язувати задачі, які лежать в основі сучасних криптографічних систем [6]. Це означає, що після створення повноцінного квантового комп'ютера більшість класичних схем розподілу ключів втратить свою стійкість [7, 8].

У цих умовах набуває особливої актуальності технологія квантового розподілу ключів (КРК) [9-11], що базується не на обчислювальній складності, а на фундаментальних законах квантової фізики [12]. Її перевага полягає у неможливості непомітного перехоплення чи копіювання квантового стану без його спотворення. Це забезпечує принципово новий рівень стійкості, недосяжний для класичних криптографічних методів.

Однак практична реалізація КРК стикається з низкою технічних і організаційних викликів [13-15]. Однією із головних проблем є обмежена довжина квантового каналу: сучасні системи забезпечують роботу на відстані до 100–150 км без використання проміжних вузлів [16]. Для побудови масштабних мереж, здатних охоплювати регіони й держави, необхідне створення багаторівневих мереж КРК зі спеціальними архітектурами, що включають довірені вузли та механізми маршрутизації ключової інформації [17-18].

Розвиток таких мереж дозволить створити інфраструктуру нового покоління для захисту критично важливих даних — у сфері державного управління, банківського сектору, оборонних та енергетичних систем. КРК може стати основою для національних і міжнародних мереж безпечного

зв’язку, забезпечивши довгострокову стійкість до атак навіть із застосуванням квантових комп’ютерів [19, 20].

Таким чином, побудова мереж квантового розподілу ключів є стратегічним завданням, яке має як наукову, так і практичну актуальність. Це напрям, що визначає рівень інформаційної безпеки майбутнього та потребує активних досліджень, стандартизації та впровадження на глобальному рівні.

Мета роботи. Метою даної роботи є розробка алгоритмів для побудови мереж квантового розподілу ключів.

Для вирішення поставленої мети вирішуються наступні **завдання**:

– проаналізувати сучасні технології генерації ключів для криптографічних перетворень;

– розробити спосіб побудови класичного автентифікованого каналу квантової апаратури;

– визначити функції універсального хешування для формування міток автентифікації;

– розробити вимоги до структури мережі КРК, рівня споживачів та рівня генерації квантових ключів;

– розробити рекомендовану структуру мережі КРК та методику побудови мережі КРК змішаної топології.

Об’єкт дослідження. Процес побудови мереж для квантового розподілу ключів.

Предмет дослідження. Алгоритми та моделі побудови мереж для квантового розподілу ключів.

Методи дослідження. Математичні методи моделювання, методи агоритмізації та програмування, методи квантового розподілу ключів.

Наукова новизна одержаних результатів.

1. Здійснено аналіз сучасних технологій генерації ключів для криптографічних перетворень та відомих способів подолання максимальної дальності під час створення квантових ключів, що дозволило обгрунтувати

опис вибраної технології та типової архітектури системи квантового розподілу ключів.

2. На основі аналіз структури мережі квантового розподілу ключів за версією ETSI розроблено алгоритм побудови автентифікованого каналу квантової апаратури та обгрунтовано варіанти використання хеш-функцій для автентифікації.

3. Згідно встановлених вимог до рівнів споживачів, генерації квантових ключів та формування квантовозахищених ключів розроблено алгоритм побудови мережі квантового розпоілу ключів.

Практичне значення отриманих результатів.

Розроблено методику побудови та рекомендовану структуру мережі квантового розпоілу ключів.

Публікації та апробація КР.

1. Сарапук О.І., Рибінський В.О., Сапіташ В.І. Архітектура системи квантового розподілу ключів. Збірник матеріалів науково-практичної конференції моодих вчених, аспірантів та студентів «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ-2025). Тернопіль, 2025. С.111-113 [21].

2. Сарапук О.І., Черняк В.А. Структура мережі квантового розподілу ключів за версією ETSI. Збірник матеріалів науково-практичного симпозіуму «Захист інформації’2025».Тернопіль, 2025. С.91-93 [22].

1 АНАЛІЗ ОСОБЛИВОСТЕЙ ГЕНЕРАЦІЇ КВАНТОВИХ КЛЮЧІВ

1.1 Аналіз сучасних технологій генерації ключів для криптографічних перетворень

У системах захищеного зв’язку дані передаються через мережі загального користування, а отже, вони доступні потенційному порушнику для проведення різних атак. Порушник може зберігати закодовані дані, що передаються каналом, а спробу декодування здійснити в майбутньому, коли нові технічні можливості та методи атак на алгоритми захисту інформації дозволять провести розкодування за прийнятний час. У цьому полягає принцип «Store now, decrypt later» («Збережи зараз, розшифруй пізніше»), що вказується як одна з основних проблем систем захисту інформації.

Водночас для відомих блочних шифрів існує параметр, що називається навантаженням на ключ, який обмежує обсяги даних, що можна обробити на одному ключі з використанням конкретного алгоритму захисту [23]. Так, рекомендації NIST [24] задають часові рамки використання ключів, які вимірюються роками.

Уповноважені органи у сфері інформаційної безпеки встановлюють набагато суттєвіші обмеження навантаження на ключ, що пов’язані з кількістю блоків, які можна обробити на одному ключі. Це обумовлено відомими атаками на блочні шифри, у тому числі через побічні канали, а також можливостями потенційного порушника залежно від класу засобу захисту інформації (ЗЗІ), у якому застосовується розглянутий алгоритм захисту. За таких обмежень виникає потреба у регулярній зміні використовуваного ключа, а отже, і пошуку варіантів доставки та/або генерації таких ключів між двома пристроями, що організовують захищений канал. Заміна ключа на новий, незалежний від попереднього, дозволяє досягти захисту передавання майбутньої інформації у разі компрометації поточного ключа.

Окремо варто відзначити занепокоєння наукової спільноти загрозою створення квантового комп’ютера. Ця технологія дозволяє ефективно

атакувати відомі схеми генерації ключів, що ґрунтуються на складності обчислення дискретного логарифма або факторизації великих чисел. Квантовий алгоритм Шора, описаний у роботах [4], [6], дозволяє вирішувати ці задачі за поліноміальний час, тому необхідно вже зараз шукати альтернативні варіанти розв’язання проблеми регулярної зміни секретного ключа у парі пристроїв.

Важливо враховувати необхідність забезпечення властивості Perfect forward secrecy (ідеальної прямої секретності), тобто у разі компрометації майстер-ключа всі наступні ключі повинні залишатися не скомпрометованими. Одним зі способів досягнення такої властивості алгоритмів кодування є періодичне оновлення майстер-ключів на нові, незалежні від раніше використаних.

Щоб запобігти накопиченню матеріалу для атак потенційним порушником та виконати вимогу навантаження на ключ, необхідно розв’язати задачу регулярної зміни цього ключа, а відповідно, регулярної доставки та/або генерації цих ключів у спареній парі пристроїв.

Відомі такі способи доставки/генерації секретного ключа:

1) доставка за допомогою довіреного кур’єра;
2) доставка за допомогою алгоритмів із секретним ключем;
3) генерація ключа за допомогою схем вироблення ключа на основі обчислювально складних задач.

Перший спосіб доставки передбачає залучення значних людських ресурсів. Більше, доставка ключового матеріалу на великі відстані потребує значного часу й, можливо, суттєвих фінансових ресурсів. Тому цей спосіб не вирішує завдання регулярної зміни секретних ключів.

Доставка ключів за допомогою алгоритмів із секретним ключем потребує попередньо розподіленого секрету. Водночас існує та сама проблема навантаження на ключ і необхідності зміни ключа захисту каналу передавання секретних ключів. Тому необхідно шукати альтернативні варіанти доставки ключів.

Використання класичних асиметричних алгоритмів, що ґрунтуються на розв’язанні складних математичних задач, також виявляється небезпечним через описані вище можливості квантового комп’ютера [25] (зокрема для застосування алгоритму Шора) та можливості порушника зберігати дані для отримання доступу до них у майбутньому, коли розвиток техніки та технологій дозволить долати раніше застосовані заходи захисту.

Серед нових технологій доставки та генерації секретних ключів можна виокремити два перспективні способи:

1) розподіл ключів за допомогою технології КРК;

2) генерація ключів між двома учасниками за допомогою постквантових алгоритмів.

Другий варіант базується на математичних задачах, складних для обчислення навіть на квантовому комп’ютері. Поточний рівень розробки таких алгоритмів є недостатнім для їх впровадження в існуючі системи. Швидкість роботи та необхідні довжини ключів цих алгоритмів не дозволяють створювати експлуатаційно виправдані зразки. Більше, існує небезпека, що після створення ефективного квантового комп’ютера з’являться нові квантові алгоритми, які дозволять ефективно розв’язувати задачі, покладені в основу постквантових алгоритмів. Такі алгоритми створять нові вектори атак на постквантові алгоритми й потребуватимуть перегляду проблеми регулярної доставки секретних ключів.

Таким чином, проблема розподілу ключів між парами користувацьких пристроїв є актуальним науковим завданням, що вимагає розв’язання в умовах появи нових загроз, пов’язаних зі створенням квантового комп’ютера. Існуючі рішення розроблялися задовго до розвитку квантових комунікацій і квантових обчислень і не враховують нових векторів атак із використанням квантових пристроїв.

Варіант розподілу ключів із використанням технології КРК виглядає найбільш перспективним для розв’язання поставленої задачі. Розподіл, а точніше, генерація ідентичних ключів на двох кінцях квантового каналу

ґрунтується на абсолютно інших фізичних принципах, що запобігає можливості проведення ефективних атак із використанням квантового комп'ютера та не дозволяє здійснювати класичні атаки з накопиченням захищених даних, як у випадку доставки ключів за допомогою алгоритмів із секретним ключем [26-28]. Водночас технологія КРК має низку суттєвих обмежень, які необхідно враховувати під час проєктування систем доставки ключів на базі КРК.

Технологія КРК дозволяє розподіляти ключі на обмеженій відстані, яка визначається використовуваним протоколом КРК та якістю квантового каналу. Для відомих протоколів КРК на InGaAs/InP лавинних фотодіодах граничною вважається відстань порядку 100 км, про що можна судити за представленими експлуатаційними характеристиками квантової апаратури [29].

Тому актуальною є задача безпечного розподілу спільного секрету для пар вузлів, що перебувають на відстані, більшій за допустиму довжину квантового каналу. Для цього вдосконалено відомий підхід побудови мереж КРК із довіреними проміжними вузлами.

Найпростішим випадком застосування КРК є використання лише двох екземплярів квантової апаратури, з'єднаних квантовим каналом, тобто використання технології в топології «точка-точка». Це базовий конструктив, з якого надалі можуть будуватися розподілені мережі з використанням КРК. Протоколи КРК для такої топології «точка-точка» активно розробляються й вивчаються науковцями. Неоціненний внесок у розвиток технології КРК зробили Ch. Bennett та G. Brassard, запропонувавши перший протокол КРК — BB84. Пристрої, що реалізують протоколи КРК, розробляються у Китаї, США, Європі [30, 31]. На жаль, більшість робіт, що стосуються протоколів КРК та квантової апаратури, присвячені фізиці процесу і не розглядають реалізацію невід'ємної частини квантової апаратури, а саме класичного автентифікованого каналу.

Будь-якій квантовій апаратурі потрібен класичний автентифікований канал. Однак існуючі наукові публікації не приділяють докладної уваги питанням інтеграції квантової апаратури й користувацьких пристроїв, ЗЗІ, для яких формуються спільні секрети. По суті, квантова апаратура генерує деяку випадкову послідовність, ідентичну з обох кінців квантового каналу та невідому порушнику. Однак існує завдання формування безпосередньо спільного секрету з такої послідовності, а також синхронізації переданих секретів у двох віддалених один від одного ЗЗІ.

Щоб подолати обмеження довжини квантового каналу апаратура КРК об'єднується у так звані мережі КРК. Однак отримання істинно квантового ключа між двома об'єктами мережі, не з'єднаними напряму квантовим каналом, потребує технології квантових повторювачів, яка на даний час далека від практичної реалізації. Питання, що стосуються створення й застосування квантових повторювачів, активно обговорюються. Поточний підхід полягає у побудові мереж КРК на основі довірених проміжних вузлів. За цього підходу квантові ключі виробляються лише між вузлами мережі, з'єднаними напряму квантовим каналом. До інших вузлів квантової мережі (ВКМ) одні квантові ключі передаються під захистом інших вироблених квантових ключів.

У мережах КРК необхідно не тільки передавати ключову інформацію з використанням квантових ключів по ланцюгу ВКМ, але й здійснювати ці процеси в мережах змішаної топології. Під змішаною топологією розуміють як топологію зв'язків ВКМ квантовими каналами, так і топологію класичних зв'язків між вузлами, наприклад, через мережу загального користування, у тому числі захищені канали взаємодії між ВКМ. При цьому граф, що відображає зв'язки квантовими каналами, має бути зв'язним. Роботи в цьому напрямі здійснюються провідними організаціями у всьому світі. У Китаї створена та успішно функціонує мережа КРК протяжністю понад 2000 км. Також ведуться роботи зі стандартизації мереж КРК, у тому числі в ETSI [32] та ITU-T. Міжнародна організація ISO займається питаннями розробки вимог із безпеки до квантової апаратури та мереж КРК. Створено європейський

проєкт OpenQKD, що передбачає розгортання випробувальних полігонів для тестування напрацювань зі створення великих мереж КРК та формування практично застосовних промислових зразків.

Нерозв’язаним залишається питання: як здійснювати розподіл спільних секретів на потрібні вузли мережі КРК, у тому числі чи існують способи уникнути появи передаваного мережею секрету у відкритому вигляді на проміжних ВКМ. Для розв’язання цього питання розробляється методика розподілу спільного секрету в мережі магістральної топології. Далі формуються вимоги до багаторівневої структури й функцій мережі КРК, на основі яких формулюється методика побудови мереж КРК змішаної топології, включаючи методику розподілу спільного секрету на довільні пари вузлів мережі.

1.2 Опис технології та типової архітектури системи квантового розподілу ключів

Технологія КРК – це технологія отримання ідентичних випадкових послідовностей двома абонентами, сформованих із використанням передачі певної інформації між цими абонентами за допомогою квантових частинок. Два абоненти застосовують спеціальну квантову апаратуру (апаратуру КРК), яка реалізує певний протокол КРК.

Протокол КРК – це протокол кодування, що включає:

- спосіб підготовки та перетворення інформаційних квантових станів в одному пристрої. Такий пристрій має містити джерело квантових станів;
- спосіб передачі інформаційних квантових станів квантовим каналом;
- спосіб перетворення, реєстрації та інтерпретації результатів вимірювань на суміжному пристрої;

– спосіб обробки послідовності, отриманої за результатами вимірювань, із використанням відкритого класичного автентифікованого каналу зв’язку. Зазвичай обробка включає етапи виправлення помилок і посилення секретності.

Метою протоколу КРК є отримання квантового ключа, ідентичного з обох боків квантового каналу.

Квантова апаратура, що реалізує протокол КРК, являє собою комплекс із двох пристроїв, з’єднаних квантовим каналом. Спрощена архітектура комплексу наведена на рисунку 1.1.

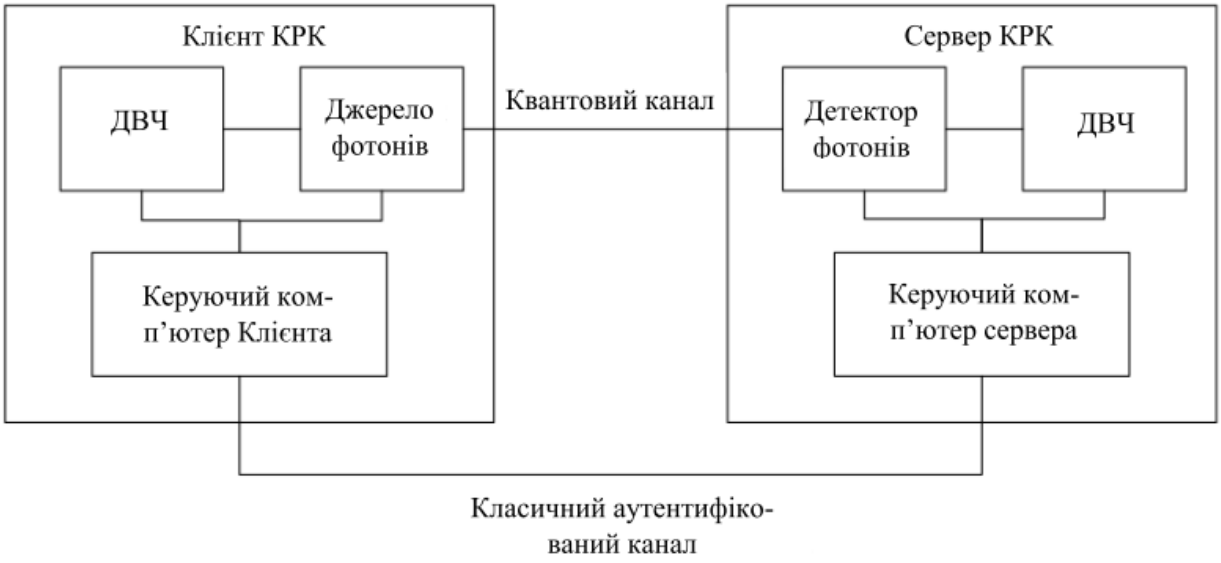

Рисунок 1.1 – Схема комплексу квантової апаратури

Один з пристроїв комплексу, що містить генератор (джерело) поодиноких фотонів, прийнято називати Клієнтом КРК. Суміжний пристрій, що містить детектор (приймач) поодиноких фотонів, називають Сервером КРК. Кожен з пристроїв має датчик випадкових чисел (ДВЧ). При цьому рекомендується використовувати датчики, в основі випадкових процесів яких лежать квантові ефекти, що дозволяє отримати істинно випадкову послідовність, з якої надалі формується квантовий ключ.

Сервер КРК і Клієнт КРК з’єднані двома логічними каналами: квантовим і класичним. Квантовий канал призначений для передачі квантових

інформаційних станів (фотонів) і зазвичай реалізується оптоволокном. Існують системи КРК, у яких як квантовий канал застосовується повітряне середовище, але вони поки що перебувають на стадії лабораторних установок. Важливою особливістю технології КРК є повна доступність квантового каналу для зловмисника, тобто цей канал не контролюється і не захищається від втручання. Крім квантового каналу, Сервер і Клієнт КРК повинні бути з'єднані класичною лінією зв'язку, де реалізується класичний автентифікований канал. До цього каналу висуваються вимоги щодо забезпечення цілісності переданих даних та автентифікації відправника.

Реальна система КРК додатково має логічний службовий канал даних, який передає команди управління й моніторингу апаратури, не пов'язані безпосередньо з протоколом КРК. У деяких реалізаціях може знадобитися забезпечення не лише цілісності, а й конфіденційності цих даних. Для роботи системи КРК в апаратуру необхідно завантажити попередньо розподілені ключі, які потрібні щонайменше для побудови класичного автентифікованого каналу до першого успішного отримання достатньої кількості квантових ключів. Одну ітерацію реалізації протоколу КРК називають сеансом КРК.
Зазвичай кожен сеанс КРК складається з таких етапів:

1) підготовка квантового каналу;
2) передача поодиноких фотонів квантовим каналом;
3) постобробка переданої послідовності.

У результаті передачі квантовим каналом обидва пристрої отримують так званий сирий ключ. Далі постобробка відбувається через класичний автентифікований канал і включає три підетапи:

1) узгодження базисів вимірювання на стороні приймача з базисами кодування на стороні джерела. Неспівпадіння відкидаються, а сирий ключ перетворюється на просіяний ключ;

2) виправлення помилок у просіяних ключах для отримання ідентичних послідовностей у Сервері та Клієнті КРК. Результат – очищений ключ;

3) посилення секретності – стиснення очищеного ключа для зменшення інформації, доступної зловмиснику. Результат – секретний квантовий ключ.

На рисунку 1.2 представлена узагальнена послідовність виконання протоколу КРК.

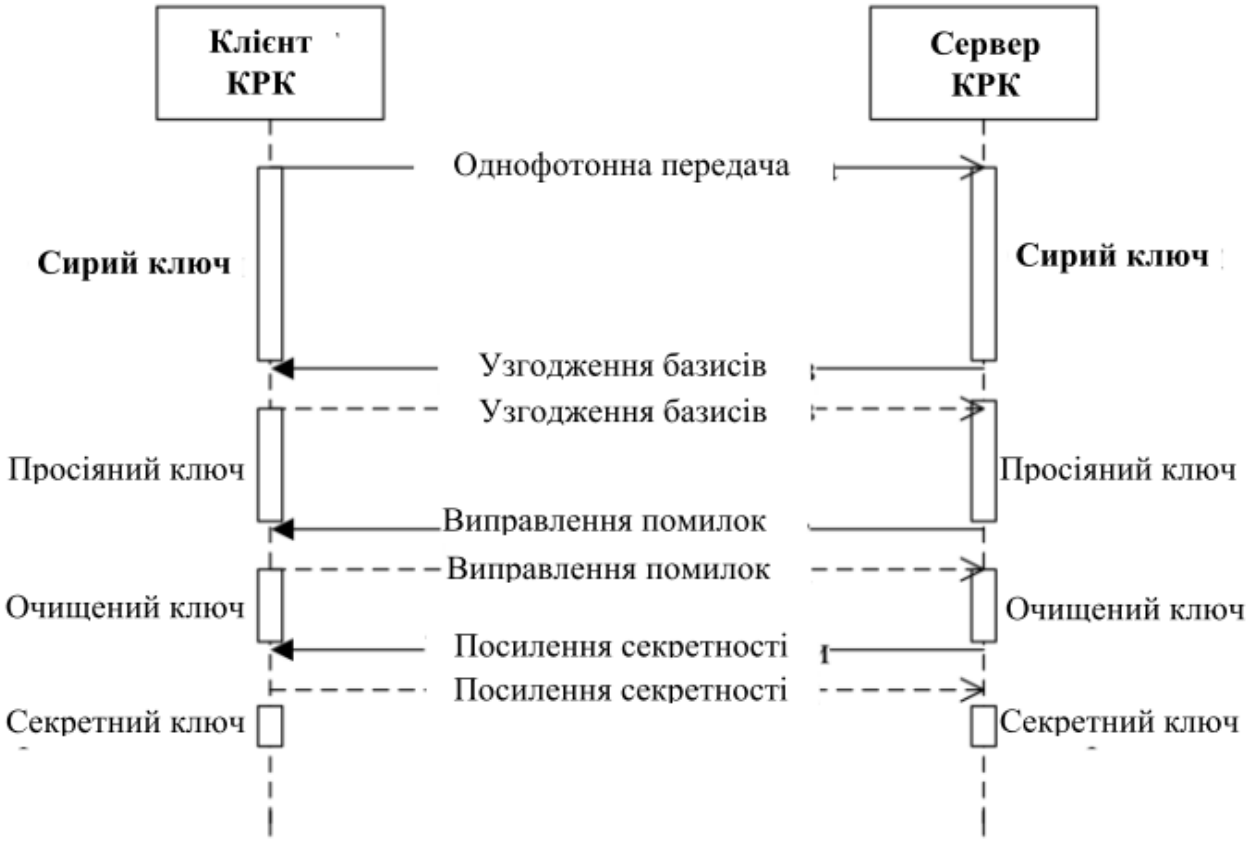

Рисунок 1.2 – Послідовність виконання протоколу КРК

Потрібно відзначити, що результат роботи квантового протоколу не зовсім коректно називати квантовим ключем. Правильніше говорити, що результатом сеансу КРК є випадкова квантова ґамма, ідентична у двох абонентів, оскільки цей результат має змінну довжину, яка не завжди збігається з довжиною ключів, що застосовуються в алгоритмах кодування. Більше того, результат виконання одного й того ж протоколу КРК суттєво відрізняється для квантових каналів із низькими та високими втратами, що безпосередньо впливають на величину помилок під час передачі в квантовому

каналі (QBER). Це, своєю чергою, впливає на обсяг інформації про квантову ґамму, доступної порушнику, і яка зменшується на етапі посилення секретності. Для стислості надалі під квантовим ключем будемо розуміти саме випадкову квантову ґамму.

Згідно з експериментальними даними, при довжині лінії у 50 км (що відповідає втратам 10 дБ при типовому затуханні у ВОЛЗ 0,2 дБ/км) ефективність вироблення квантових ключів, тобто відношення числа зареєстрованих імпульсів на сервері КРК до загальної кількості імпульсів, відправлених клієнтом КРК, становить 2×10^{-5}. Таким чином, щоб отримати 256-бітний квантовий ключ при довжині лінії 50 км за один сеанс КРК, потрібна послідовність у 2×10^{7} імпульсів. Втрати при довжині квантового каналу у 100 км складають 20 дБ, тобто у 10 разів більше, ніж при 50 км. Тому для вироблення 256-бітного квантового ключа за один сеанс КРК послідовність імпульсів, що передається квантовим каналом, має бути в 10 разів більшою, тобто не менше, ніж 2×10^{8} імпульсів.

Оцінимо обсяг випадкових чисел, необхідний для одного сеансу КРК, у результаті якого має утворитися квантовий ключ довжиною не менше 256 біт. Довжина 256 біт обрана як типова для стандартизованих алгоритмів із секретним ключем. Для кодування інформаційного стану протоколу КРК потрібно мінімум 2 біти інформації:

- один біт визначає базис кодування або базис вимірювання;
- другий біт безпосередньо задає значення переданого інформаційного біта 0 або 1.

Більш складні протоколи КРК, наприклад протокол ГОКС на геометрично однорідних когерентних станах, можуть мати 3 і більше біти для кодування інформації в однофотонному стані. Виходячи з експериментальних даних, для одного сеансу КРК необхідна випадкова послідовність довжиною не менше 4×10^{8} біт. Оцінимо знизу необхідну швидкість генерації випадкових чисел для отримання 256-бітного ключа за секунду. Нехай існує ідеальний протокол КРК, який за одну секунду перетворює всі імпульси у квантовий

ключ. Тоді швидкість роботи ДВЧ повинна становити не менше 4×10^8 біт/с або 400 Мбіт/с. Якщо враховувати, що частина квантового ключа використовується для автентифікації наступного сеансу КРК, то фактична швидкість генерації квантових ключів повинна також включати необхідний розмір ключа автентифікації, що підвищує нижню межу вимог до швидкості ДВЧ.

До датчиків випадкових чисел у системах КРК висуваються суворі вимоги, які стосуються природи випадковості й відповідно якості формованої послідовності. Водночас швидкість фізичних датчиків, у основі яких лежать квантові процеси, є обмеженою, що призводить до обмеження граничних швидкостей вироблення квантових ключів саме швидкістю доступних ДВЧ.

Таким чином, для коректного функціонування протоколу КРК і отримання квантових ключів належної якості необхідно забезпечити передачу інформації квантовим каналом, побудувати класичний автентифікований канал, мати датчик випадкових чисел відповідної якості як джерело ентропії для створюваних квантових ключів.

Багато теоретичних робіт, що описують фізичну сторону технології КРК, не приділяють належної уваги побудові класичного автентифікованого каналу. Для створення такого каналу необхідно визначити спосіб забезпечення цілісності даних і автентифікації джерела даних. Типовим рішенням є обчислення імітовставки для переданих повідомлень, що дозволяє перевіряти їхню цілісність. Автентифікація відправника даних при цьому здійснюється за рахунок використання секретного ключа, відомого лише парі легітимних абонентів.

Широко поширеним способом обчислення імітовставки є застосування обчислювально стійких хеш-функцій. У ряді робіт рекомендується використання функцій універсального хешування як функцій для формування імітовставки в класичному автентифікованому каналі систем КРК. Водночас функції універсального хешування потребують значно більшої кількості ключового матеріалу для створення однієї імітовставки. Вважається, що

квантового ключа, сформованого в результаті одного сеансу КРК, повинно вистачати і для автентифікації наступного сеансу, і для формування корисного секрету, який передається абонентам.

Слід враховувати, що квантова апаратура не використовується сама по собі, а виступає джерелом спільних секретів для користувацьких пристроїв і засобів захисту інформації (ЗЗІ). Класичний автентифікований канал із різних причин, наприклад для економії кількості фізичних каналів між пристроями, може бути реалізований через користувацькі ЗЗІ. Невирішеним науковим питанням при цьому залишається спосіб забезпечення автентифікації каналу.

Крім того, під час роботи квантової апаратури потрібно враховувати, що можливі як одноразові, так і багаторазові переривання сеансу КРК через порушення цілісності даних у класичному автентифікованому каналі внаслідок дій зловмисника або випадкових збоїв. Кожен повторний запуск сеансу КРК призводить до додаткових витрат ключів автентифікації.

Іншою важливою науковою проблемою, яка не розглянута в науковій літературі, є власне передача сформованого квантового ключа від квантової апаратури абонентам, а точніше — користувацьким пристроям, які будуть цей квантовий ключ використовувати. На відміну від класичних систем, взаємодія квантової апаратури із ЗЗІ відбувається одночасно у двох парах пристроїв: Сервер КРК – ЗЗІ та Клієнт КРК – ЗЗІ.

Квантовий ключ створюється в одній парі пристроїв (квантова апаратура), а повинен потрапити в іншу пару пристроїв ЗЗІ. При цьому, на відміну від класичних систем, небезпечно застосовувати алгоритми, які не є стійкими до атак із використанням квантового комп’ютера.

Можливості безпечної взаємодії географічно віддалених пристроїв також обмежені. Такі пристрої можуть мати лише попередньо розподілений ключ для організації захищеної взаємодії або, що ще гірше, не мати жодного первинного спільного ключа. Формування спільних секретів користувацьких пристроїв асиметричними методами є небезпечним через атаки з використанням квантового комп’ютера.

Науковою проблемою є також досягнення синхронізації переданої в ЗЗІ ґами в описаних умовах таким чином, щоб пара суміжних ЗЗІ використовувала гарантовано ідентичні спільні секрети, а також могла їх однозначно ідентифікувати.

Таким чином, можна перелічити низку нерозв'язаних наукових проблем у розподілі спільних секретів із використанням КРК у топології «точка-точка»:

- спосіб організації класичного автентифікованого каналу апаратури КРК, включно зі способом формування імітовставки для забезпечення цілісності та джерелом ключів для її створення;
- організація захищеної передачі спільних секретів у ЗЗІ, стійкої до атак квантовим комп'ютером;
- необхідність синхронізації переданої у пару ЗЗІ ключової ґами в умовах відсутності можливості взаємодії цих ЗЗІ до отримання первинних ключів.

Розв'язання окреслених наукових проблем дозволить застосовувати технологію КРК для систем у топології «точка-точка» з метою регулярного розподілу спільних секретів у користувацькі пристрої.

1.3 Аналіз відомих способів подолання максимальної дальності створення квантових ключів

Усі протоколи КРК мають граничну довжину квантового каналу, на якій можливе створення квантових ключів. У середньому максимальна довжина квантового каналу для волоконних систем КРК становить 100 км. Проте користувацькі пристрої, яким необхідно розподіляти спільні секрети, розташовуються довільно. У зв'язку з цим постає завдання подолання максимальної віддаленості пристроїв квантової апаратури з метою створення спільних секретів для пар пристроїв із необмеженою відстанню між ними.

Першими кроками у вирішенні цієї проблеми можна вважати створення спеціальних протоколів КРК, що використовують один недовірений

проміжний вузол – або Сервер КРК, або Клієнт КРК. До таких протоколів належать MDI-QKD та Twin-Field QKD. Основна ідея цих протоколів полягає в тому, що абоненти використовують два екземпляри квантової апаратури одного типу (два Сервери КРК чи два Клієнти КРК), кожен з яких є довіреним вузлом і з’єднаний із проміжним недовіреним вузлом іншого типу. Спеціальна структура протоколу КРК дозволяє без кодування квантових інформаційних станів на проміжному недовіреному вузлі надати кожному абоненту достатньо інформації для формування сирого ключа. У результаті застосування подібних протоколів у середньому вдвічі збільшується максимальна відстань між абонентами, що отримують секретний ключ, оскільки фактично існують два квантові канали, кожен з яких не повинен перевищувати максимальної довжини, визначеної протоколом КРК.

На жаль, такі протоколи не розв’язують завдання створення спільного секрету для двох довільно розташованих абонентів, а лише забезпечують подвоєння максимальної дальності.

Наступним кроком у вирішенні проблеми максимальної віддаленості абонентів є використання одного з двох підходів: застосування мереж КРК на основі довірених проміжних вузлів та застосування мереж КРК на основі недовірених проміжних вузлів. У кожному випадку йдеться про мережі змішаної топології, у яких необхідно мати можливість розподіляти спільний секрет на довільні пари вузлів мережі.

В основі мереж КРК із множиною недовірених проміжних вузлів лежить використання заплутаних фотонів і комірок квантової пам’яті, розташованих на проміжних вузлах. Наразі квантова пам'ять є абстрактним об'єктом без фізичного втілення, тому мережі КРК із недовіреними вузлами є перспективним, але поки що нереалізованим підходом.

В основі мереж КРК із довіреними проміжними вузлами закладена ідея послідовної передачі певного квантового ключа, отриманого на сегменті мережі, через проміжні вузли до цільових вузлів, яким необхідно передати спільний секрет. Далі всі вузли такої мережі КРК будемо називати вузлами

квантової мережі (ВКМ). Ця система з урахуванням розглянутих проблем є базовим блоком побудови мереж КРК із довіреними проміжними вузлами та мінімальним сегментом такої мережі.

Відомий підхід конкретизує один зі способів розподілу спільного секрету шляхом використання одного з квантових ключів, отриманого на деякому сегменті мережі. Цей квантовий ключ призначається спільним секретом для кінцевих ВКМ. У теоретичній моделі передача спільного секрету на кінцеві ВКМ здійснюється послідовною передачею по ланцюжку ВКМ із захистом на квантових ключах відповідного сегмента. При цьому на кожному проміжному вузлі відбувається перекодування спільного секрету, і він з'являється у відкритому вигляді, що вимагає, аби ВКМ були довіреними. Як алгоритм кодування зазвичай застосовується одноразовий шифроблокнот (One-Time Pad Encryption).

Описаний спосіб формування спільного секрету для магістральної мережі з чотирьох ВКМ представлений на рисунку 1.3.

Нехай є мережа КРК із вузлів ВКМ1, ВКМ2, ВКМ3, ВКМ4. Вузли ВКМ1 та ВКМ4 цільові, між ними необхідно сформувати загальний секрет. Спочатку між парами ВКМ виробляються квантові ключі КК12, КК23, КК34. Потім загальним секретом пари цільових ВКМ призначається один із вироблених квантових ключів, наприклад, ключ КК12. Він уже є на ВКМ1, тепер необхідно доставити його на ВКМ4. Для цього на ВКМ2 отримують закодований текст шляхом кодування ключа КК12 на ключі КК23 Закодований текст передається на ВКМ3, розкодується на ключі КК23. Тепер на ВКМ3 теж є КК12.

Аналогічно КК12 передається з ВКМ3 на ВКМ4 в закодованому вигляді. Як ключ кодування використовується КК34. Розкодувавши отриманий закодований текст на ВКМ4 за допомогою ключа КК34 отримують КК12. Таким чином на обох кінцевих ВКМ є загальний ключ КК12, який використовується як загальний секрет для передачі з мережі КРК зовнішнім пристроям.

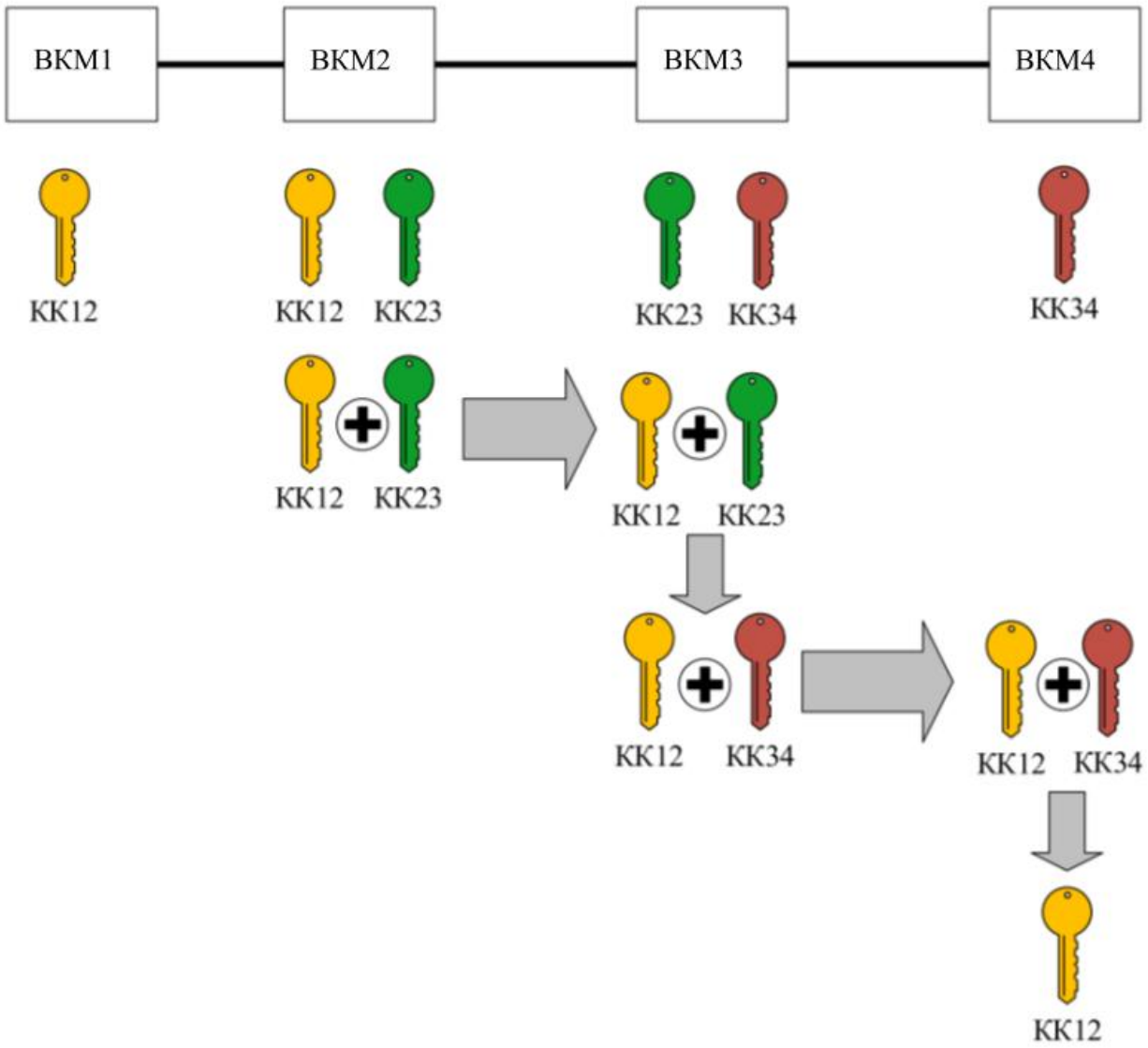

Рисунок 1.3 – Базовий спосіб формування секретного ключа через ланцюжок ВКМ

Істотним недоліком пропонованого підходу під час передачі ключа є рішення лише завдання забезпечення конфіденційності передачі, але не цілісність ключа. Крім того, пропонується використовувати квантовий ключ деякого сегмента, тобто. ключ, про який у порушника є деяка, нехай мала інформація. Також переданий ключ у явному вигляді з'являється на кожному проміжному вузлі. Використання одноразового шифроблокноту передбачає одноразове застосування квантових ключів, що тягне за собою суттєву витрату квантових ключів кожного сегмента. Таким чином, відомий базовий підхід

може розглядатися як початковий крок при синтезі способів розподілу загального секрету для довільних УКБ, але вимагає подальшого опрацювання та усунення описаних недоліків.

Одним із відомих варіантів вирішення проблеми появи ключової інформації у відкритому вигляді на проміжних ВКМ є спосіб, який показує застосування строго стандартизованих класичних методів для захищеного подання ключової інформації на проміжних ВКМ. Для розуміння вказаного способу розглянемо схему магістральної мережі КРК, представленої на рисунку 1.4.

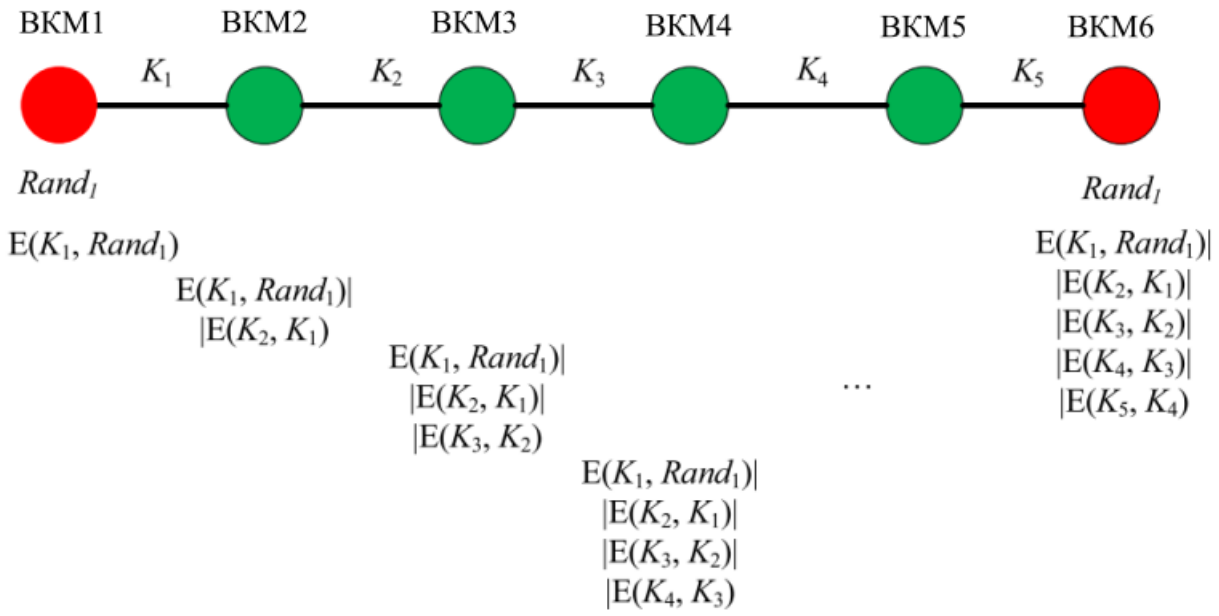

Рисунок 1.4 – Спосіб передавання секретного ключа «матрьошкою»

Для захисту безпосередньо ключової інформації $Rand_1$, призначеної загальним секретом цільових ВКМ, використовується квантовий ключ першого сегмента K_1 мережі КРК. Формується закодований текст C_1 = E(K_1, $Rand_1$). Даний закодований текст передається по ланцюжку вузлів до другого цільового ВКМ, тобто до ВКМ6. Для розкодування на ВКМ6 необхідний квантовий ключ K_1. Він передається від ВКМ2 мережі КРК із захистом на квантовому ключі K_2, тобто C_2 = E(K_2, K_1). Формування і передавання C_i

продовжується доти, доки не буде переданий передостанній квантовий ключ K_4, закодований на квантовому ключі останнього сегмента K_5.

Тепер цільовий ВКМ6 може у зворотному порядку розкодувати всі отримані закодовані тексти, у результаті чого отримає передану ключову інформацію $Rand_1$.

Слід зауважити, що попри відсутність вимог до функції кодування, необхідно застосовувати незалежний набір квантових ключів для кожної магістральної підмережі КРК, виділеної в певній мережі КРК змішаної топології, навіть при перетині на деяких сегментах кількох магістральних підмереж. Інакше передавані спільні секрети різних підмереж КРК будуть мати зв'язок через ключі захисту, використані під час кодування на перехресних сегментах.

Водночас, якщо достатньо забезпечувати обчислювальну стійкість під час розподілу спільного секрету цільових ВКМ, то для виділеної магістральної підмережі КРК передавання ключів захисту спільного секрету по сегментах необхідно здійснити лише один раз, а потім можна сформувати кілька закодованих текстів C_1 від кількох повідомлень X для формування кількох спільних секретів. Допустима кількість різних закодованих текстів на одному ключі першого сегмента залежить від допустимого навантаження на ключ кодування для конкретного обраного алгоритму кодування.

Як видно з наведеного опису, додавання нових ВКМ у ланцюжок між цільовими ВКМ суттєво збільшує обсяг передаваної захищеної інформації при спробі не допустити появи передаваних КЗК на проміжних ВКМ у відкритому вигляді класичними методами.

Перевагами даного способу є:

– відсутність перекодування передаваних спільних секретів на проміжних ВКМ, що вирішує проблему появи спільних секретів на проміжних ВКМ у відкритому вигляді;

– теоретико-інформаційна стійкість захисту при передаванні ключів за умови використання відповідних алгоритмів кодування та суворо одноразового застосування квантових ключів;

– можливість скорочення кількості передаваних закодованих текстів під час формування обчислювально стійких спільних секретів для фіксованої магістральної підмережі КРК з метою підвищення швидкості розподілу спільних секретів.

Водночас суттєвим недоліком способу є пропорційне збільшення обсягу передаваних закодованих повідомлень від кількості сегментів у мережі КРК.

Існує інший спосіб, заснований на схемах поділу секрету. Підсумковий спільний секрет розділяється на частки певною схемою поділу секрету, після чого доставляється до цільових ВКМ різними ланцюжками ВКМ. У результаті порушникові необхідно отримати доступ до множини УКС з різних ланцюжків, щоб здобути доступ до спільного секрету.

Таким чином, визначено основу способів генерації клчів і спостерігаються спроби усунути основні недоліки. Проте вдосконалення способу на даний момент потребує доопрацювання.

2 ПОБУДОВА АВТЕНТИФІКОВАНОГО КАНАЛУ ДЛЯ КВАНТОВОЇ ГЕНЕРАЦІЇ КЛЮЧІВ

2.1 Аналіз структури мережі КРК за версією ETSI

Наразі ведуться роботи у сфері стандартизації мереж КРК у частині архітектури таких мереж та способів їх функціонування.

Група стандартизації ETSI у сфері квантового розподілу ключів (ISG QKD) з 2010 року почала розробляти стандарти, що стосуються технології КРК, базуючись на результатах добре відомого проєкту SECOQC (Secure Communication based on Quantum Cryptography). Ці стандарти охоплюють різні сфери застосування КРК: безпеку протоколів і реалізацій КРК, інтерфейси взаємодії, методи вимірювань тощо. Багато стандартів і специфікацій, розроблених у 2010 році, наразі переглядаються та доповнюються.

Перший варіант мережі КРК був представлений у описі інтерфейсу взаємодії квантової апаратури та СЗІ. Мережа КРК побудована з довірених вузлів, як показано на рисунку 2.1.

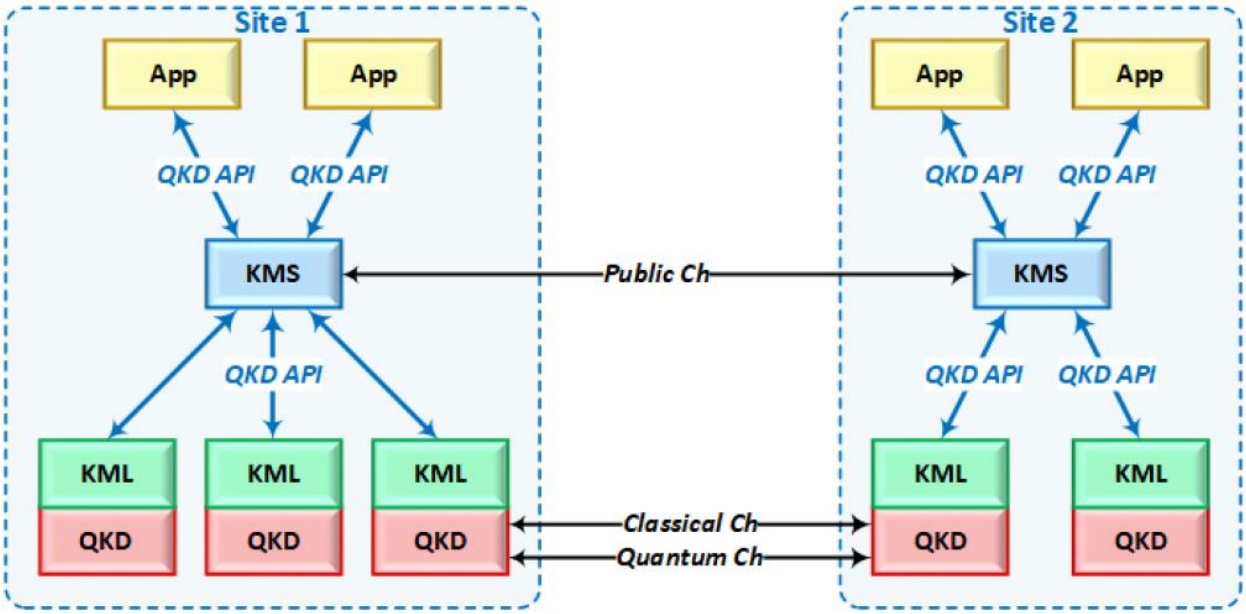

Рисунок 2.1 – Структура мережі КРК за документом ETSI GS QKD 004

У сценарії взаємодії відповідно до ETSI GS QKD 004 беруть участь:

- апаратне забезпечення КРК – QKD;
- сервер управління квантовими ключами – KML;
- сервер управління ключами – KMS;
- клієнти мережі, користувацькі застосунки – App.

Система побудована з незалежних частин. Довірений вузол містить кілька екземплярів квантової апаратури, сервери управління квантовими ключами, сервер управління ключами. При цьому до довіреного вузла включається також користувацький застосунок, для якого генеруються секретні ключі.

Далі проводиться аналіз кожного з об’єктів довіреного вузла та його функцій.

З досвіду проєкту європейської мережі SECOQC базовим елементом мережі КРК є квантова апаратура. При цьому сполучені пари комплектів квантової апаратури, з’єднані як квантовим каналом, так і класичним автентифікованим каналом, є самодостатнім елементом. Генерація квантових ключів відбувається повністю незалежно від інших процесів у мережі КРК.

Як віомо, квантова апаратура генерує не ключ, а випадкову послідовність нефіксованої довжини. Для формування квантових ключів із сукупності випадкових послідовностей застосовуються сервери управління квантовими ключами (KML). На кожен блок квантової апаратури в кожному ВКМ припадає по одному серверу управління квантовими ключами. Ця частина ВКМ формує квантові ключі з послідовностей, отриманих від квантової апаратури, зокрема присвоюючи ідентифікатори квантових ключів та іншу метаінформацію. Сервер управління квантовими ключами містить сховище квантових ключів, у яке поміщаються сформовані квантові ключі з усією необхідною метаінформацією. При цьому ідентичність квантових ключів, згенерованих у двох сусідніх вузлах, ґрунтується лише на довірі до протоколу КРК, що теоретично гарантує ідентичність сформованих послідовностей.

Для передавання спільних секретів у СЗІ-споживачі, закріплені за ВКМ, не з’єднаними безпосередньо квантовим каналом, використовується сервер управління ключами (KMS). Цей елемент ВКМ у ранніх документах ETSI описаний поверхнево, без зазначення способу розподілу спільного секрету між несусідніми вузлами. З досвіду проєкту SECOQC можна припустити, що застосовується підхід, описаний раніше (див. рис. 1.3), який полягає у передаванні квантового ключа з певного сегмента мережі на цільові ВКМ. Як захист передавання квантового ключа використовується кодування одноразовим блокнотом. Як показано на рисунку 2.1, канали зв’язку для формування спільного секрету відокремлені від класичного каналу апаратури КРК. Питання забезпечення цілісності під час передавання квантового ключа не розглядається.

Мережа КРК допускає підключення багатьох СЗІ до одного вузла. При цьому вперше вводиться вимога щодо розміщення СЗІ та інших елементів ВКМ в одній контрольованій зоні.

Таким чином, перший варіант мережі КРК за версією ETSI являє собою чотирирівневу структуру. Два рівні мережі оперують квантовими ключами, третій рівень призначений для передавання квантових ключів, згенерованих на одному сегменті мережі КРК, на інші сегменти. Четвертий рівень мережі – рівень користувацьких застосунків. Другий рівень мережі досить чисельний за кількістю елементів, кожен з яких виконує лише невелику частину функцій, реалізованих у ВКМ, і може бути оптимізований. Третій рівень, навпаки, є найбільш навантаженим елементом ВКМ. Включення четвертого рівня до складу УКС виглядає не зовсім коректним рішенням. Без споживача ключів мережа КРК і її УКС можуть функціонувати. Користувацькі пристрої потрібні саме як зовнішні по відношенню до мережі КРК елементи.

Наразі стандарт ETSI GS QKD 004 V1.1.1 переглядається та готується нова версія.

Пізніше був випущений стандарт ETSI GS QKD 014 V1.1.1, у якому внесено суттєві зміни до опису структури мережі КРК. Схематичне зображення мережі КРК наведено на рисунку 2.2.

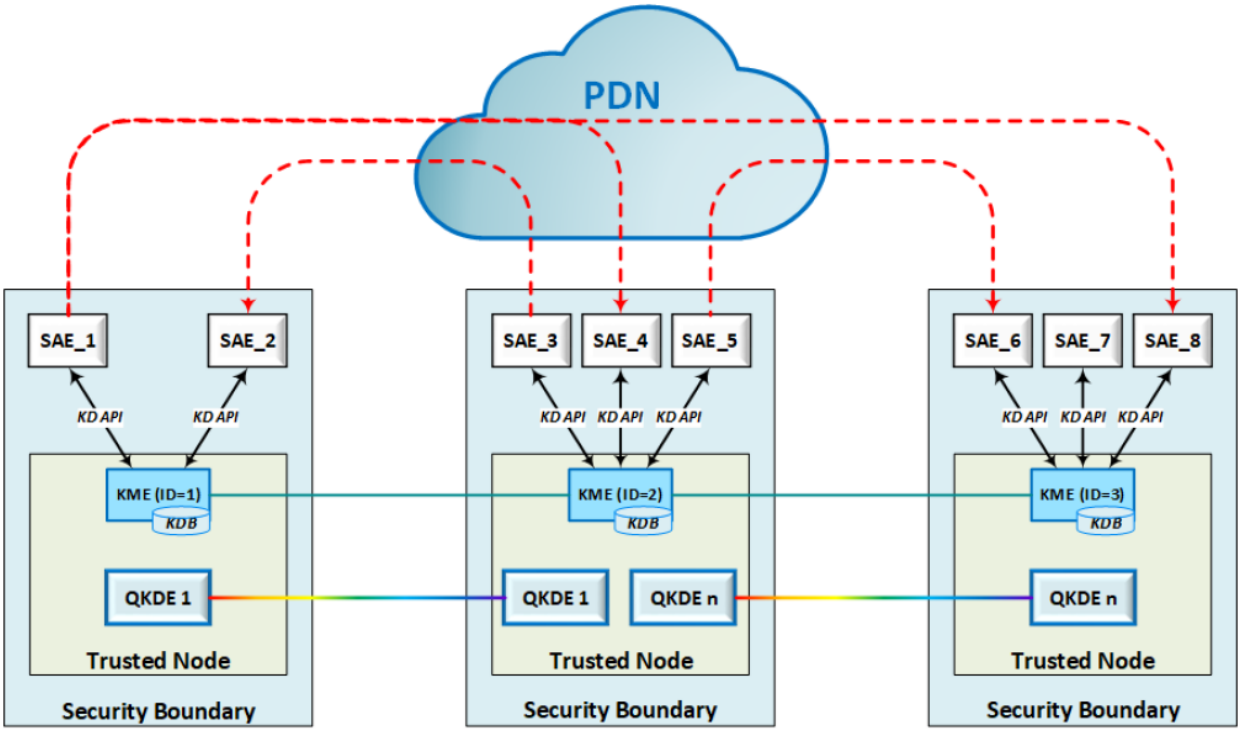

Рисунок 2.2 – Структура мережі КРК згідно з ETSI GS QKD 014

У сценарії роботи мережі КРК беруть участь:

- апаратне забезпечення КРК – QKDE;
- сутність управління ключами – KME;
- клієнти мережі – SAE.

Як видно з рисунка 2.2, відбулося суттєве спрощення структури мережі шляхом об’єднання сервера управління квантовими ключами та сервера управління ключами в єдиний об’єкт. При цьому СЗІ винесені за межі ВКМ, але водночас повинні розташовуватися в межах контрольованої зони для забезпечення безпеки передавання секретних ключів у СЗІ.

Довіреним вузлом називається вузол, що містить у собі і пристрій управління ключами KME, і клієнт мережі SAE. При цьому інтерфейс взаємодії описується з таких припущень:

– вузол працює та управляється безпечно;

– KME і SAE перебувають у межах одного вузла;

– інтерфейс взаємодії не виходить за межі контрольованої зони довіреного вузла;

– KME є безпечним;

– SAE є безпечним;

– KME має мати унікальний ідентифікатор у межах мережі КРК;

– SAE має мати унікальний ідентифікатор у межах мережі КРК.

Таким чином, початкова структура мережі містила чотири рівні, розділяючи управління квантовими ключами та формування спільних секретів згідно з запитами користувацьких застосунків. При цьому користувацькі застосунки включалися до складу довірених вузлів мережі, що не зовсім коректно.

У наступній версії структури мережі цей недолік був виправлений: користувацькі застосунки були винесені за межі мережі, тобто вони користуються мережею КРК як сервісом для отримання спільної секретної інформації. Водночас таке спрощення структури вузла шляхом об’єднання блоків управління квантовими ключами та взаємодії з користувацькими застосунками ускладнює вузол мережі, оскільки майже всі функції вузла концентруються в єдиному блоці мережі, який і раніше був найбільш навантаженим в ВКМ.

В обох версіях мережі КРК не розглядаються способи розподілу спільного секрету для користувацьких застосунків, а також питання захисту каналів взаємодії вузлів та управління вузлами мережі. Для другої версії мережі КРК додані абстрактні вимоги щодо безпеки вузлів мережі, які не сприяють спрощенню побудови мережі КРК загалом і довірених вузлів зокрема.

2.2 Спосіб побудови класичного автентифікованого каналу квантової апаратури

Можна виділити два основних підходи до забезпечення автентифікації даних у класичному каналі. Квантові ключі, що виробляються в результаті протоколу КРК, володіють стійкістю в теоретико-інформаційному сенсі. Першим підходом є використання автентифікації того ж класу стійкості, оскільки стійкість усієї системи визначатиметься за стійкістю її найменш захищеного елемента. Альтернативним підходом є використання автентифікації, стійкої у обчислювальному сенсі, щодо якої на сьогодні не існує ефективних реалізованих атак). У цьому випадку досягається обчислювальна стійкість автентифікації класичного каналу, при цьому можлива економія ключа автентифікації із збереженням обчислювальної стійкості використовуваного протоколу, але відбувається зниження класу стійкості квантових ключів до обчислювально стійких.

2.2.1 Універсальне хешування як спосіб обчислення імітовставки

Як автентифікація, стійка у теоретико-інформаційному сенсі, для систем КРК розглядаються функції універсального хешування. Клас функцій універсального хешування H визначається такими вимогами:

1) кількість хеш-функцій із H, таких, що довільне повідомлення $m_1 \in M$ (M – простір повідомлень) відображається у довільну мітку $t_1 \in T$ (T – простір міток автентифікації), і в точності дорівнює $|H|/|T|$;

2) кількість функцій із H, які відображають довільне повідомлення $m_1 \in M$ у довільну мітку $t_1 \in T$ і при цьому відображають довільне повідомлення $m_2 \neq m_1 \in M$ у деяку мітку $t_2 \in T$ (можливо, рівну t_1), не перевищує $\varepsilon|H|/|T|$, де $\varepsilon > 1/|T|$.

Такий клас хеш-функцій називається класом ε–ASU$_2$-функцій (Almost Strong Universal Hashing). Параметр ε є параметром стійкості класу хеш-функцій.

2.3 Варіанти використання хеш-функцій для автентифікації

Для побудови автентифікованого каналу з метою забезпечення цілісності переданих даних необхідно виробляти мітку автентифікації (імітовставку) з використанням універсальних хеш-функцій. Мітка автентифікації повідомлення t може бути отримана кількома способами:

1) $t=h_{kj}(m_j)$, де m_j – j-те автентифіковане повідомлення, h_{kj} – хеш-функція, що відповідає ключу автентифікації k_j. Кожен ключ k_j використовується для автентифікації лише одного повідомлення;

2) $$t = \begin{cases} h_{kj}\left(m_0^j\right), j = 0,1,2,... \\ h_{kj}\left(m_i^j\right) + k^j_{opt_i}, j = 0,1,2,...; i = 1,2,3... \end{cases}.$$

У цьому випадку кожна хеш-функція використовується більше одного разу. Після першого застосування h_{kj} наступні мітки автентифікації від повідомлень m_{ij} кодуються одноразовим шифроблокнотом на ключах k^j_{otpi}, де j – порядковий номер використаної функції хешування, яка відповідає ключу k^j, $\left\{m_i^j\right\}, i = 0,1,2,...$ - набір повідомлень, для аутентифікації яких використовується одна функція хешування;

3) $t = h_{kj}\left(m_i^j\right) + k^j_{opt_i}, j = 0,1,2,...; i = 0,1,2,...$. У цьому варіанті всі результати застосування хеш-функції h_{kj} до автентифікованого повідомлення кодуються одноразовим шифроблокнотом на ключі k^j_{otpi}.

Варіанти 2 і 3 дозволяють економити ключ автентифікації, оскільки довжина закодованої мітки автентифікації, а отже й ключа одноразового шифроблокнота, менша, ніж довжина ключа функції універсального хешування. Проте відома ефективна атака на варіанти 1 і 2, а також необхідність кодування одноразовим шифроблокнотом усіх міток автентифікації, включно з першою.

Таким чином, найбільш доцільним варіантом обчислення мітки автентифікації з використанням універсальних хеш-функцій є варіант 3.

2.4 Функції універсального хешування для формування міток автентифікації

Для формування міток автентифікації можна використати такі функції універсального хешування:

1) сімейство функцій Wegman-Carter. Їх параметри такі:

$$|M|=2^i,\ |T|=2^j,\ j<i,\ p \text{ – найменше просте число, } p > 2^i. \quad (2.1)$$

Хеш-функція обчислюється згідно такої формули:

$$f_{(q,r)}(m) = ((mq + r) \bmod p) \bmod |T|, \quad (2.2)$$

де q, r – секретні параметри (ключ хеш-функції), які однозначно визначають хеш-функцію з сімейства хеш-функцій $H_1=\{f_{(q,r)}: q\in Z_p\backslash\{0\}, r\in Z_p\}$ – сімейство SU_2 хеш-функцій.

Для даного сімейства хеш-функцій оптимальними з точки зору використання ключів є довжина повідомлень $2L$ і довжина виходу хеш-функції L визначаються так:

$$L=l_t+\log_2 \log_2 l_m, \quad (2.3)$$

де $l_t=\log_2|T|$ – довжина мітки автентифікації;

$l_m=\log_2|M|$ – довжина повідомлення.

Обчислення міток аутентифікації від довільнх повідомлень за допомогою сімейства функцій Wegman-Carter відбувається таким чином.

Формується H_1 – сімейство хеш-функцій з максимальною довжиною оброблених повідомлень $l'_m=2L$ і довжиною виходу хеш-функцій L. Параметр L визначається за формулою (2.3).

Аутентифіковане повідомлення m ділиться на блоки довжини $2L$, які хешуються в блоки довжиною L із застосуванням $f_{(q1,\ r1)}$. Маємо $\left\lceil \frac{\log_2|M|}{2L} \right\rceil$ блоків. Блоки, отримані в результаті застосування хеш-функції, конкатенуються в проміжний рядок m_1.

Проміжний рядок m_1 ділиться на блоки довжини $2L$, які хешуються в блоки довжини L із застосуванням $f_{(q2,r2)}$.

Процес повторюється на різних хеш-функціях H (тобто з використанням різних ключів для кожного раунду хешування) до тих пір, поки не залишиться останній блок довжини L. Ключем для вибору хеш-функції є пара (q_i, r_i).

Молодші t біт цього останнього блоку – шукана мітка аутентифікації t.

Сукупна довжина ключів, необхідних для ідентифікації всіх використовуваних хеш-функцій, становить $4L \cdot \log_2 l_m$. Під ключем розуміється конкатенація ключів для всіх використаних хеш-функцій

Стійкість хеш-функції $2/T - ASU_2$;

2) сімейство функцій Stinson [94]. Її параметри хешування взначаються таким чином:

$$q=2,\ s=l_t+\lceil \log_2 \log_2 l_m \rceil,\ i = \lceil \log l_m/s \rceil,\ p=q^s,\ M=M_1{}^{2i},\ T=T_2,\ |M|=2^{lm},\ |T|=2^{lt}. \quad (2.4)$$

Сімейство функцій хешування будується на основі двох допоміжних функцій.

Перша допоміжна функція хешування описується формулою:

$$g_x: M_1 \rightarrow T_1,\ g_x(y, z)=xy+z, \quad (2.5)$$

де $M_1 = F_p \times F_p$ – простір хешованих повідомлень;

$T_1=F_p$ – простір виходів хеш-функції;

$x, y, z \in F_p$.

Сімейство універсальних хеш-функцій G_1, побудоване на допоміжній хеш-функції (2.5) має вигляд:

$$G_1=\{g_x: x\in F_p\}. \quad (2.6)$$

Дане сімейство може бути розширене до сімейства $M_1{}^{2^j}$ для всіх j=1, 2, … , i . У цьому випадку маємо таку хеш-функцію:

$$h^{2^j}: M^{2^j}\rightarrow T^{2^j};\ h^{2^j}(m_1, \ldots, m_{2^j})=(h(m_1), \ldots, h(m_{2^j})),\ h\in G_1. \quad (2.7)$$

І відповідно сімейство хеш-функцій буде мати вигляд:

$$G_1{}^{2^j}=\{h^{2^j}: h\in G_1. \quad (2.8)$$

Послідовно застосовуючи функції сімейства $G_1{}^{2^j}$ для всіх $j = i, \ldots, 1$, отримуємо мітку аутентифікації довжини p із повідомлення довжиною p^{2^i}. Таким чином отримується клас функцій $G_1{}^{2^j}$, що складається з p^i хеш-функцій, які хешують повідомлення з $M_1{}^{2^i}$ в мітки аутентифікації з T_1.

Друга допоміжна функція хешування представляється так:

$$g_{xy}: M_2\rightarrow T_2,\ z\rightarrow\varphi(xz)+y, \quad (2.9)$$

де $M_2=F_{qs}$, $T_2=F_{qt}$ - параметри функції хешування;

$\varphi(x)=\varphi((x_1, \ldots, x_s))=(x_{i1}, \ldots, x_{ilt})$ – деяке відображення наборів довжини s в набори довжини l_t.

Клас SU хеш-функцій має такий вигляд:

$$G_2=\{g_{xy}: (x, y)\in F_{qs}\times F_{qt}\}. \quad (2.10)$$

Підсумкове сімейство хеш-функція виходить шляхом комбінування сімейств G_1^{2i} та G_2.

Обчислення міток автентифікації від довільних повідомлень з допомогою сімейства функцій Stinson проводиться наступним чином.

Мітка автентифікації виходить за i+1 раундів.

На перших i раундах значення, що хешується, доповнюється нулями до довжини, кратної $2s$. Значення повідомлення хешується функцією з G_1^{2j}, де j – номер раунду, застосовується функція g_{kj}, де k_j – ключ для j-го раунду.

На останньому раунді застосовується функція $g_{ka,kb}$ з G_2, де k_a, k_b – ключі для хеш-функції.

Довжина ключа для ідентифікації всіх необхідних хеш-функцій дорівнює $(\log_2 l_m - \log_2 l_t+2)l_t$.

Стійкість хеш-функції $2/|T| - ASU_2$;

3) сімейство функцій den Boer. Для їх генерації вважаємо, що $|M|=n\cdot l_m$, тобто повідомлення $m \in M$ розбивається на n підповідомлень $m_i \in GF(2^t)$. Хеш-функція має вигляд:

$$h_{k_1,k_2}(m) = k_1 + \sum_{i=1}^{n} m_i k_2^i . \qquad (2.11)$$

Тоді сімейство хеш-функцій представляється у такому вигляді:

$$H = \left\{ h_{k_1,k_2} : k_1, k_2 \in GF\left(2^{l_t}\right) \right\}. \qquad (2.12)$$

Довжина ключа для ідентифікації всіх необхідних хеш-функцій $2l_t$. Стійкість хеш-функції $\frac{|M|}{|T|\log_2|T|} - ASU_2|M|$. Слід відмітити, що стійкість функції хешування істотно залежить від вибору максимальної довжини повідомлень, що обробляються;

4) сімейство функцій Bierbrauer (з урахуванням кодів Ріда-Соломона). Для формування функції аутентифікації будується $[n,\ k,\ d]_q$ код. Його параметри задовольняють такому співвідношенню:

$$n=2^{l_t}+s,\ k=1+2^s,\ d=n-k+1=2^{l_t+s}-2^s,\ q=2^{l_t+s}, \tag{2.13}$$

де s – мінімальне ціле, таке що $l_m<(l_t+s)(1+2^s)$, тоді $s\approx\lceil\log_2 l_m-\log_2 l_t\rceil$.

Потужність простору оброблюваних повідомлень для хеш-функції, побудованої на такому коді, становитиме $|M| = 2^{(l_t+s)(1+2^s)}$.

Аутентифікація за допомогою сімейства функції Bierbrauer здійснюється в такий спосіб. Вибирається $k_1\in\{0,1\}^{n+s}$ – ключ універсальної хеш-функції.

Вибираються $k_a\in\{0,1\}^{n+s}$, $k_b\in\{0,1\}^n$ – ключі для хеш-функції з G_2 згідно формули (2.10).

Повідомлення доповнюється нулями до довжини, кратної l_t+s і розбивається на блоки довжини l_t+s. Кожен j-ий блок множиться на $k_1^{(j-1)}$ для всіх j = 1, … , i , після чого всі результати множень додаються. Множення та піднесення до степеня відбувається у полі $F_2{}^{r+s}$.

На останньому раунді застосовується функція $g_{ka,kb}$ з G_2.

Довжина ключа для ідентифікації всіх необхідних хеш-функцій $3l_t+2s$.

Стійкість хеш-функції $2/|T|-ASU_2$;

5) матриці Тепліца. Нехай A – матриця Тепліца з a рядками та b стовпцями. Нехай $y\in T$.

Тоді функція хешування повідомлення m має вигляд:

$$h_{(A,\ y)}\colon M\to T;\ t=h_{(A,\ y)}(m)=Am+y. \tag{2.14}$$

Довжина ключа для ідентифікації всіх необхідних хеш-функцій l_m+2l_t-1.

Стійкість такої хеш-функції $1/|T|-ASU_2$.

Зауважимо, що для хешування кожного нового повідомлення необхідна побудова нової матриці Тепліца. Отже, ключ функції хешування може перевищувати довжину повідомлення, що хешується, так як для побудови матриці потрібен обсяг випадкових даних, що перевищує розмір аутентифікованого повідомлення. У таблиці 2.1 наведено ключові параметри та особливості розглянутих функцій хешування.

Таблиця 2.1 – Порівняльна таблиця параметрів функцій хешування

	ε	Довжина ключа	Примітка
Wegman-Carter	$\frac{2}{\lvert T\rvert}$	$4(t+\log_2\log_2 l_m)\cdot$ $\cdot\log_2 l_m$	Фіксоване значення ε
Stinson	$(\log_2 l_m-\log_2 l_t+$ $+1)/\lvert T\rvert$	$(\log_2 l_m-\log_2 t+2)l_t$	Малий розмір ключа
der Boer	$\frac{\lvert M\rvert}{\lvert T\rvert\log_2\lvert T\rvert}$	$2l_t$	Найменший розмір ключа
Bierbrauer	$\frac{2}{\lvert T\rvert}$	$3l_t+2(\log_2 l_m-\log_2 l_t)\approx$ $\approx 3l_t+2\log_2 l_m$	Фіксоване значення ε. Малий розмір ключа.
Матриці Тепліца	$\frac{1}{\lvert T\rvert}$	$2l_t+l_m-1$	Матриці Тепліца не можна використати при умові зміни ключа для кожного аутентифікованого повідомлення.

В таблиці 2.1 розглядаються ключові параметри, що визначають експлуатаційні властивості, а саме: параметр стійкості ε та загальну довжину ключа, необхідну для аутентифікації повідомлення m довжини l_m.

Типовим джерелом ключа для функції аутентифікації класичного автентифікованого каналу в системах КРК для деякого (не першого) сеансу КРК є частина квантового ключа, виробленого на попередньому сеансі КРК. Якщо застосовувати функції аутентифікації з мінімальною необхідною довжиною ключа, то більша частина квантового ключа одного сеансу КРК може бути використана для передачі абонентам.

Як видно з наведеної таблиці 2.1, найменшими розмірами ключів володіють функції сімейств Stinson, der Boer, Bierbrauer. Однак, використання сімейства функцій Bierbrauer пов'язані з побудовою коду Ріда-Соломона великої розмірності, а стійкість сімейства функцій der Boer значно залежить від довжини оброблюваних повідомлень. Найбільш доцільним є застосування функцій сімейства Stinson. При малій витраті ключа вони володіють простотою конструкції та параметром стійкості, що залежить всього від логарифму довжини оброблюваних повідомлень.

Фундаментальною проблемою теоретико-інформаційно стійкої аутентифікації є необхідність використання нових різних незалежних ключів аутентифікації для кожного аутентифікованого повідомлення. Нагадаємо, що як ключ для аутентифікації наступної сесії вироблення квантових ключів прийнято використовувати частину від загального квантового ключа, виробленого внаслідок поточного протоколу КРК.

Таким чином, в залежності від обсягів переданих даних, які необхідно аутентифікувати на етапах роботи протоколу КРК, можлива ситуація, при якій більша частина виробленого квантового ключа буде витрачена на аутентифікацію каналу для наступної серії. Нижня оцінка для довжини ключа аутентифікації таких функцій – двійковий логарифм від довжини повідомлення.

Покажемо необхідний обсяг ключа автентифікації для одного сеансу КРК. Можна виділити кілька підходів для автентифікації повідомлень, що з'являються на етапі постобробки протоколу КРК:

1) мітка аутентифікації обчислюється від кожного повідомлення при первинній передачі його в класичному каналі, що аутентифікується. Цей метод найбільш витратний за необхідним розміром ключа аутентифікації, оскільки довжина ключа аутентифікації пропорційна логарифму довжини автентифікованих повідомлень. Проводити розрахунки для цього методу недоцільно;

2) мітка автентифікації обчислюється від усіх повідомлень, переданих протягом одного етапу сеансу КРК в один бік (тільки у бік Клієнта КРК та лише у бік Сервера КРК окремо) наприкінці кожного етапу. Тобто необхідно виділити шість ключів автентифікації певної довжини;

3) мітка автентифікації обчислюється від усіх повідомлень в обидві сторони (у сторону Клієнта КРК та у бік Сервера КРК разом), переданих протягом одного етапу сеансу КРК;

4) мітка автентифікації обчислюється один раз від усіх повідомлень, переданих протягом трьох етапів протоколу КРК після закінчення сеансу КРК.

Розрахуємо нижню оцінку необхідних розмірів ключів автентифікації для запропонованих підходів. Розрахунок зроблений на основі обсягів даних, що передаються в класичному автентифікованому каналі, для комплексу ViPNet Quandor. Довжина квантового каналу складає 100 км і довжина квантового ключа, що одержується в результаті одного сеансу КРК, дорівнює 256 біт. На етапі узгодження базисів обсяг даних від Сервера КРК у бік Клієнта КРК і назад склав відповідно m_1=m_2=1920 біт. На етапі виправлення помилок - m_3=1056000 біт і m_4=256 000 біт. На етапі посилення таємності – m_5=2256000 біт та m_6=12000 біт.

У загальному випадку довжина необхідного ключа аутентифікації обчислюється за формулою:

$$k_j = \sum_i \log_2 m_i \,, \tag{2.15}$$

де i – номер автентифікованого повідомлення;

m_i – довжина аутентифікованого повідомлення;

j – номер підходу аутентифікації.

Для підходу аутентифікації 4 маємо такий загальний обсяг даних в обидві сторони дорівнює: $m=\sum m_i=3583840$ біт.

Тоді довжина ключа аутентифікації, згідно (2.15) набуває значення: $k_4=\log_2 m\approx 22$ біта.

Для підходу аутентифікації 3 маємо відповідно такі обсяги даних, що аутентифікуються: $m_1'=m_1+m_2=3840$ біт; $m_2'=m_3+m_4=1312000$ біт; $m_3'=m_5+m_6=2268000$ біт. Тоді довжина ключа аутентифікації згідно (2.15) дорівнює: $k_3=\log_2 m_1'+\log_2 m_2'+\log_2 m_3'\approx 55$ біт.

Для підходу аутентифікації 2 згідно (2.15) маємо таку довжину ключа аутентифікації: $k_2=\sum\log_2 m_i\approx 97$ біт.

Уточнимо отримані оцінки для довжин ключів аутентифікації. Згідно оцінок довжини ключа автентифікації, для них найменшою довжиною володіє хеш-функція на базі коду Ріда-Соломона. Для неї довжина ключа обчислюється за формулою:

$$k'=2\log_2 m+3t, \qquad (2.16)$$

де t - довжина мітки аутентифікації,

m - довжина аутентифікованого повідомлення.

Відповідно до рекомендацій SECOQC довжина мітки аутентифікації має бути не менше 64 біт.

Таким чином, маємо наступні оцінки довжин ключа аутентифікації згідно (2.16) відповідно: $k_2'=1346$ біт, $k_3'=686$ біт, $k_4'=236$ біт.

Розрахунки для підходу аутентифікації 1 не проводилися через те, що цей підхід ще більш витратний, ніж підхід аутентифікації 2. Згідно здійсненим розрахункам обсягів даних та результуючої довжини квантового ключа

випливає, що для квантового каналу завдовжки 100 км очікується вироблення 400 біт квантового ключа внаслідок виконання одного сеансу КРК. Таким чином, тільки підхід аутентифікації 4 потенційно можливий: кількість біт, необхідних на ключ аутентифікації, менша, ніж число біт одержуваного квантового ключа. Однак за такого підходу аутентифікації залишиться всього 164 біти квантового ключа, який можна використовувати для організації захищеного каналу взаємодії. Якщо під час розрахунку довжини ключа аутентифікації приймати, що за один сеанс КРК виробиться 256 біт квантового ключа, то жоден із запропонованих підходів не дозволить виділити частину квантового ключа в якості ключа аутентифікації, і необхідно застосовувати альтернативний метод доставки ключів аутентифікації до квантової апаратури для забезпечення потреб у ключах аутентифікації множини сеансів КРК

Таким чином, при розглянутих швидкостях виробітку квантових ключів 256 біт за сеанс КРК неможливе застосування аутентифікації, що має теоретико-інформаційну стійкість.

Недостатній обсяг квантового ключа, тобто необхідність витрачати весь або більшу частину квантового ключа на автентифікацію наступного сеансу, обумовлений ступенем стиснення очищеного ключа на етапі посилення таємності. Ступінь стиснення етапу посилення секретності залежить від величини помилки в квантовому каналі та, відповідно, розміру даних, що передаються на етапі виправлення помилок та розкривають порушнику інформацію про вироблений квантовий ключ. Для конкретної системи, використаної для розрахунку, можливе зменшення фактичної довжини квантового каналу, що призведе до зменшення помилки у квантовому каналі та, відповідно, зменшення ступеня стиснення на етапі посилення таємності.

Загалом, для систем КРК, які мають недостатню швидкість генерації квантових ключів через високий рівень стійкості вироблених квантових ключів (високого ступеня стиснення на етапі посилення таємності), застосування теоретико-інформаційно стійкої аутентифікації виявляється неможливим. Для таких систем необхідне застосування обчислювально

стійкої аутентифікація. При цьому, на відміну від першого підходу, на одному ключі аутентифікації допустимо аутентифікувати кілька повідомлень до вичерпання допустимого навантаження на ключ відповідної функції автентифікації.

У цьому випадку для аутентифікації класичного каналу використовується імітовставка,. Довжина ключа автентифікації складає 256 біт. При цьому, на відміну від теоретико-інформаційно стійкого підходу, на одному ключі автентифікації обчислюються мітки аутентифікації від множини повідомлень у межах допустимого навантаження на ключ аутентифікації. У кожному з цих підходів кожен вироблений квантовий ключ диверсифікується на ключ аутентифікації та ключ кодування, який буде використано для передачі зовнішнім пристроям. В якості систем КРК функція диверсифікації тривіальна і полягає у розбитті виробленого квантового ключа KK на ключі для користувачів $K_{\text{кор}}$ та ключі аутентифікації $K_{\text{аут}}$ наступного сеансу КРК відповідного розміру згідно обраної функції аутентифікації (рисунок 2.3).

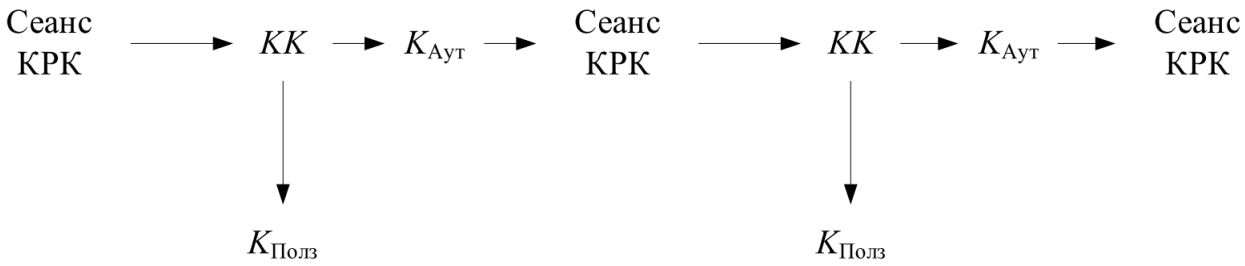

Рисунок 2.3 – Схема диверсифікації квантових ключів протоколу КРК

Таким чином, у системах КРК з високим ступенем стиснення на етапі посилення секретності неможливе застосування теоретико-інформаційно стійкої автентифікації з урахуванням необхідного обсягу ключів автентифікації універсальних хеш-функцій. При цьому зберігається можливість застосування обчислювально стійких способів аутентифікації при побудові класичного автентифікованого каналу для таких систем через

фіксований розмір ключа аутентифікації незалежно від обсягу даних, що аутентифікуються.

У той же час, якщо ступінь стиснення на етапі посилення таємності дозволяє отримати необхідний обсяг ключа для формування ключа автентифікації, то рекомендується застосування універсальних функцій хешування для збереження теоретико-інформаційної стійкості вироблюваних квантових ключів. Функції універсального хешування, побудовані за принципом Stinson, мають мінімальний необхідний розмір ключа серед функцій універсального хешування з фіксованим показником стійкості.

3 АЛГОРИТМ ПОБУДОВИ МЕРЕЖІ КРК

3.1 Розроблення вимог до структури мережі КРК

Мережа КРК описується за рівневою моделлю. Рівнева модель дозволяє розділити складну систему на прості елементи з обмеженим і чітко визначеним функціоналом, що сприяє повному та зрозумілому опису системи, а також дає змогу здійснювати незалежну розробку її частин різними виробниками. За аналогією з досвідом побудови класичних мереж, проєктування мережі КРК здійснюється з урахуванням того, що нижчі рівні надають ресурси для використання вищими рівнями. Такий принцип, зокрема, закладений у мережевій моделі ISO/OSI.

У процесі аналізу закордонних проєктів мереж КРК та квантової апаратури, яка реалізує протоколи КРК, було виявлено таке:

1) квантові ключі**,** що генеруються квантовою апаратурою, є випадковими послідовностями нефіксованої довжини, причому ця довжина може змінюватися від сеансу до сеансу генерації ключів. Необхідно забезпечити формування квантових ключів із випадкових послідовностей з урахуванням можливих випадкових або навмисних збоїв під час їх формування, зберігання та передавання;

2) мережа КРК в СЗІ надає КЗК. Такі ключі розподіляються по певному ланцюгу ВКС, який можна розглядати як підмережу магістральної топології. Необхідно визначити спосіб формування такого ланцюга, а також метод розподілу КЗК по обчисленій траєкторії;

3) керування процесом генерації квантових і КЗК може здійснюватися як локально, так і віддалено — централізовано або децентралізовано. Потрібно визначити оптимальний спосіб такого керування;

4) взаємна автентифікація ВКС, їхніх складових частин і взаємодія із зовнішніми СЗІ потребують додаткового опрацювання. Звичні методи побудови великих класичних мереж тут непридатні через неможливість

використання методів узгодження спільного ключа та автентифікації вузлів, що базуються на обчислювально складних математичних задачах.

Централізована система керування та контролю мережі КРК є менш надійною, ніж децентралізована. Подібний центр керування виступає потенційною точкою відмови всієї мережі. Натомість, якщо функції керування розподілені між вузлами ВКС, то вихід із ладу одного вузла призведе до зупинки роботи лише певного сегмента мережі, а не всієї системи.

Аналіз проєктів мереж КРК, а також потенційних споживачів технології показує, що зовнішні СЗІ необхідно підключати не до всіх ВКС. У мережі КРК з’являються проміжні вузли, що виконують лише функцію подовження квантового каналу, а не джерела ключів для зовнішніх користувачів. Отже, доцільно виділити змінну частину ВКС, яка відповідає за взаємодію із зовнішнім СЗІ-споживачем, в окремий рівень мережі. У результаті деякі ВКС можуть мати спрощену структуру без функції видачі КЗК.

Пропонується три рівні побудови мережі КРК:

- рівень генерації квантових ключів;
- рівень генерації КЗК;
- рівень керування КЗК (рівень взаємодії із зовнішнім споживачем).

Додатково для подальших пояснень вводиться рівень споживачів, який представлений парами СЗІ-споживачів, у тому числі не об’єднаних в єдину мережу. Рівень споживачів є зовнішнім щодо мережі КРК. У зарубіжних джерелах його часто називають рівнем застосувань (application layer).

Таким чином, мережу КРК можна подати як сукупність взаємопов’язаних рівнів, як це показано на рисунку 3.1.

При введенні трирівневого поділу мережі КРК з'являються три інтерфейси взаємодії між рівнями:

- інтерфейс між квантовою апаратурою та керуючим СЗІ (рівнем вироблення КЗК) - інтерфейс передачі квантових ключів;

- внутрішній інтерфейс вузла мережі КРК між рівнем вироблення КЗК та рівнем управління КЗК - інтерфейс довіреного вузла;

- інтерфейс між Мережею КРК та Споживачем – інтерфейс із мережею КРК.

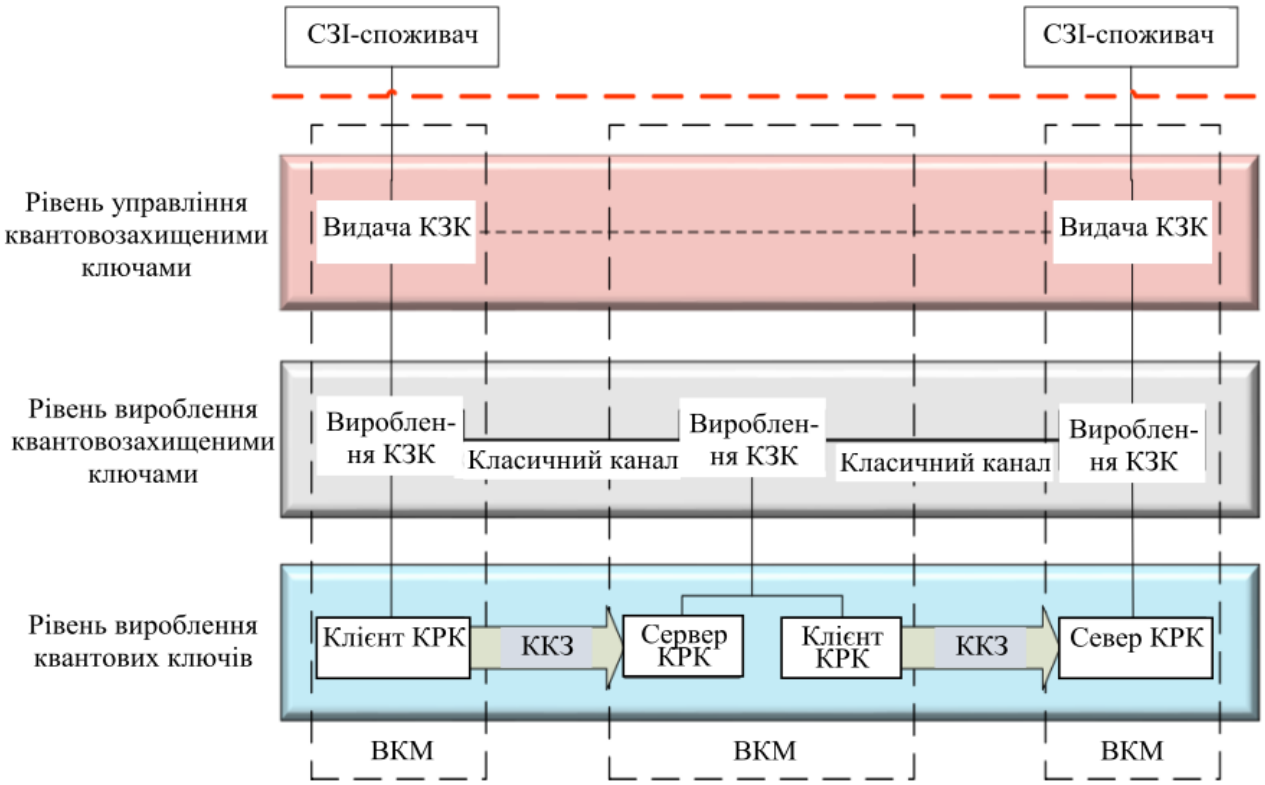

Рисунок 3.1 – Структура мережі КРК (по рівнях)

На рисунку 3.2 представлені інтерфейси взаємодії між різними рівнями мережі.

Варто зазначити, що рівень вироблення квантовозахищених ключів сам по собі є СЗІ, так як здійснює вироблення та зберігання ключової інформації, а також її використання для забезпечення конфіденційності, цілісності та автентичності даних у мережі КРК.

Квантова апаратура, що безпосередньо виробляє квантові ключі, може бути реалізована різними виробниками, заснована на різних протоколах КРК, але для пропонованої мережі КРК така варіативність не повинна мати значення. Мережа КРК повністю має працювати незалежно від конкретної реалізації пар квантової апаратури Таким чином, інтерфейс взаємодії між квантовою апаратурою та СЗІ є базовим для реалізації будь-якої мережі КРК.

Для подібної взаємозамінності необхідне опрацювання стандарту взаємодії між квантовою апаратурою та зовнішнім обладнанням.

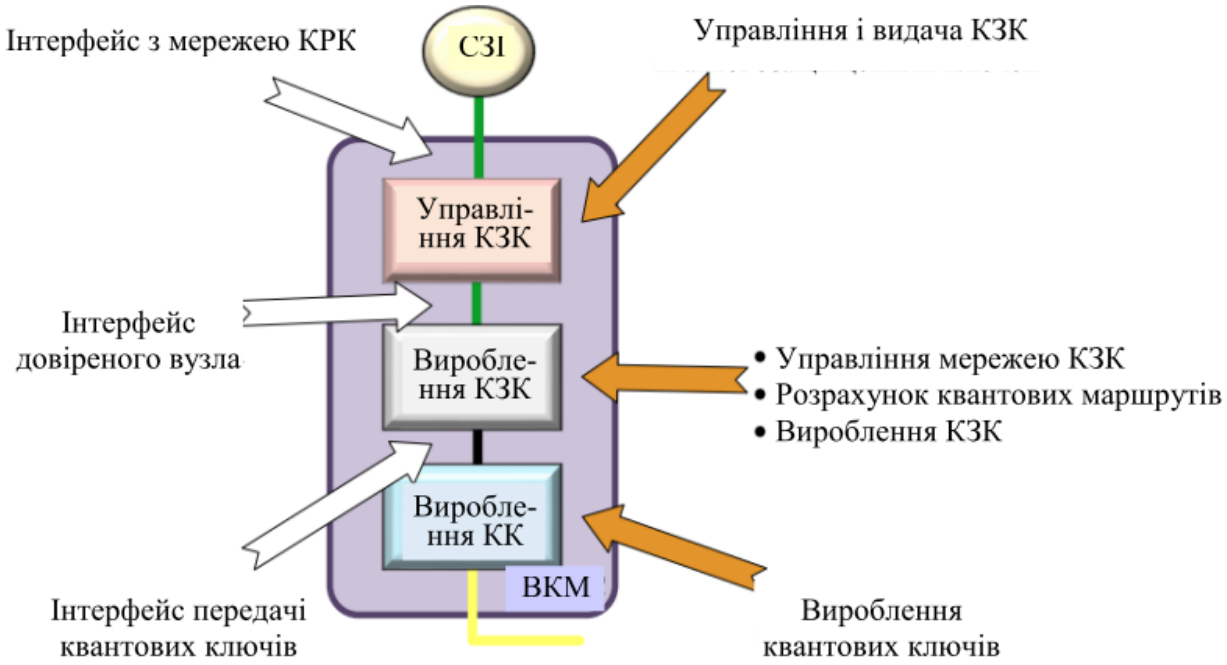

Рисунок 3.2 - Інтерфейси взаємодії між різними рівнями мережі

Інтерфейс внутрішньої взаємодії ВКМ між рівнем вироблення та рівнем управління КЗК – це інтерфейс між нерозривно пов'язаними частинами ВКМ. Метою цього інтерфейсу є обмеження доступу із зовнішньої мережі до внутрішніх процесів мережі КРК. Необхідний контроль за реалізованим функціоналом цього інтерфейсу. При цьому, на відміну від двох інших інтерфейсів, які з'єднують об'єкти, потенційно здатні працювати незалежно один від одного та виготовляються різними виробниками, цей інтерфейс не вимагає опрацювання стандартизованої взаємодії між модулями двох рівнів.

Останній інтерфейс – інтерфейс зв'язку з кінцевим споживачем. Як і інтерфейс із квантовою апаратурою, він вимагає розробки стандарту взаємодії, тому що реалізує взаємодію об'єктів множини різних виробників. А з погляду споживача має здійснюватись підтримка довільної мережі КРК.

3.2 Вимоги до рівня споживачів та рівня генерації квантових ключів

Рівень споживачів складається із СЗІ, які мають функцію отримання КЗК від мережі КРК. Важливою особливістю мережі КРК є те, що кожен споживач повинен мати можливість підключатися до будь-якого ВКС, який містить модуль рівня керування КЗК.

СЗІ-споживачі можуть бути пов’язані з іншими СЗІ-споживачами незалежно від мережі КРК. Споживачі повинні здійснювати захищену передачу даних відповідно до таких зв’язків.

Два СЗІ-споживачі можуть бути підключені як до різних вузлів мережі КРК, так і до одного й того ж вузла.

Метою СЗІ-споживача при взаємодії з мережею КРК є отримання КЗК для обміну з іншим, пов’язаним із ним СЗІ-споживачем. При цьому СЗІ-споживач повинен знати ідентифікаційну інформацію свого пов’язаного споживача, але може не знати, до якого саме вузла мережі КРК він підключений.

Можливі різні варіанти контролю легітимності запитів на отримання КЗК від ЗЗІ-споживачів:

- на рівні споживачів: СЗІ-споживачі самостійно визначають, із ким можуть встановлювати зв’язок, а мережа КРК виконує запити без перевірки їх легітимності;
- на рівні мережі КРК: споживач надсилає запит на отримання КЗК, а мережа самостійно перевіряє, чи має він відповідні права.

Доцільно виконувати перевірку легітимності запитів саме на рівні мережі КРК, що дозволяє запобігти компрометації переданих спільних секретів у разі, якщо зловмисник отримає доступ до одного із СЗІ-споживачів.

Слід зазначити, що ЗЗІ-споживач може бути як стаціонарним (постійно підключеним до мережі КРК), так і мобільним (здатним змінювати вузол підключення). Тому необхідно забезпечити можливість зміни вузла прив’язки ЗЗІ до мережі.

Рівень генерації квантових ключів являє собою попарно з’єднані модулі квантового обладнання. На кінцях кожного сегмента обов’язково повинна бути апаратура одного виробника (принаймні доти, доки не буде уніфіковано протоколи КРК і відповідні оптичні схеми).

Існують кілька підходів до функціонування цього рівня в частині керування квантовими каналами та взаємної ідентифікації модулів мережі КРК. Один із підходів передбачає умовно автономне квантове обладнання**,** яке самостійно організовує автентифікований канал, здійснює адресацію під час передавання даних між своїми екземплярами та самостійно керує квантовими каналами, включно з їх комутацією. У цьому випадку рівень генерації квантових ключів повинен:

- розраховувати обсяг запитів на квантові ключі;
- визначати допустиму частоту запитів залежно від характеристик (використовуваного протоколу КРК, якості та довжини квантового каналу тощо);
- здійснювати узгоджене перемикання квантових каналів відповідно до сукупності запитів.

Такий підхід значно ускладнює роботу «фізичного» рівня мережі КРК.

Згенерований квантовий ключ передається на наступний рівень — рівень формування квантовозахищених ключів.

Інший підхід передбачає винесення управління комутацією каналів на вищий рівень мережі КРК. У цьому випадку модулі рівня генерації квантових ключів працюють попарно, а побудова квантового каналу переноситься на рівень формування КЗК.

Квантова апаратура працює за топологією «точка-точка», тому їй байдуже, яким способом і яким обладнанням надано квантовий канал. Вищий рівень регулює запити на ключі, забезпечуючи необхідні умови для їх успішного виконання. Оптичний комутатор керується з центру підмережі топології «зірка».

Природа квантового протоколу забезпечує синхронне отримання квантових ключів на обох кінцях каналу (ключ або є з обох боків, або його немає). Ситуація, коли ключ отримано лише з одного боку, неможлива.

Перед передаванням квантових ключів на вищий рівень потрібно сформувати ключі з випадкової послідовності, присвоїти їм ідентифікатори та метадані, а також здійснити перевірку ідентичності перед збереженням у сховище. У мережі КРК рекомендується зберігати квантові ключі на вищому рівні, який використовує їх як ресурс для виконання своїх функцій.

Модулі генерації квантових ключів мають зв’язок через квантовий і класичний канали. Класичний канал доцільно реалізовувати через модулі верхнього рівня для спрощення адресації даних у мережі КРК.

3.3 Вимоги до рівня формування квантовозахищених ключів

Другий рівень мережі КРК є найбільш навантаженим за кількістю функцій. У подальшому розвитку мереж можуть бути виділені додаткові рівні — наприклад, для прогнозування навантаження на сегменти мережі залежно від нерівномірності запитів на ключі.

На цьому рівні відбуваються два основні процеси:

1) керування генерацією квантових ключів;
2) безпосереднє формування КЗК.

Модуль цього рівня відповідає за формування запитів на квантові ключі та забезпечення класичного каналу між сусідніми вузлами мережі (якщо це необхідно). Після генерації квантових ключів і передачі їх у модулі формування КЗК потрібно забезпечити їх збереження з відповідними метаданими (ідентифікатор, довжина, час створення, сегмент тощо). Рекомендується, щоб інтерфейс передачі квантових ключів підтримував контроль синхронної видачі ключів з обох кінців каналу.

Рівень КЗК також повинен забезпечувати управління допоміжним обладнанням (наприклад, оптичними комутаторами), необхідним для роботи

рівня генерації квантових ключів. Далі цей рівень обробляє запити від рівня керування квантовозахищеними ключами. Отримавши запит із зазначенням цільового УКС, модуль КЗК визначає та резервує ланцюг УКС, через який буде здійснюватися формування КЗК.

Ланцюг обирається на основі метрик сегментів мережі (кількість наявних ключів, швидкість генерації, швидкість використання тощо). Маршрут резервується, щоб запобігти конкуренції ресурсів між іншими процесами.

Після визначення маршруту виконується розподіл КЗК, після чого сформований ключ передається для зберігання та подальшого використання.

Для обробки запитів на розподіл КЗК необхідно:

1) побудувати та підтримувати актуальну топологію мережі КРК;

2) визначити ланцюг ВКМ за допомогою алгоритму пошуку шляху у зваженому графі;

3) виконати розподіл КЗК згідно з обраним методом;

4) забезпечити контроль цілісності та ідентичності ключів.

Для забезпечення взаємодії між модулями сусідніх вузлів достатньо використовувати квантові ключі. Для зв’язку між модулями несусідніх вузлів потрібні попередньо розподілені або службові КЗК. Необхідна уніфікована система ідентифікації вузлів, щоб модуль КЗК міг однозначно визначити цільовий ВКМ.

Розрахунок ланцюга для розподілу КЗК виконує вузол, який ініціював запит. Якщо ланцюг стає недоступним (розрив каналу, збій вузла тощо), він має бути перерахований. У разі зміни метрик сегмента або появи конфліктів резервів ланцюг оновлюється. Модулі мають оперативно інформувати один одного про зміни, щоб мережа могла найефективніше виконувати запити на КЗК.

Для цього доцільно передбачити прямі зв’язки між вузлами на основі попередньо розподілених або службових ключів.

3.4 Рекомендована структура мережі КРК

В результаті аналізу процесів, що відбуваються в мережі КРК, та вимог до функцій рівнів мережі запропоновано рекомендовану структуру мережі КРК тавимоги до її функцій. Структура мережі КРК у вигляді вузлів і зв'язків між ними представлено рисунку 3.3. Використовуються такі позначення: ККЗ – квантовий канал зв'язку; КАК - Класичний автентифікований канал; КА – квантова апаратура.

Також визначені модулі рівня управління квантовозахищеного ключа (КЗК), рівня виробітку КЗК, рівня виробітку квантових ключів.

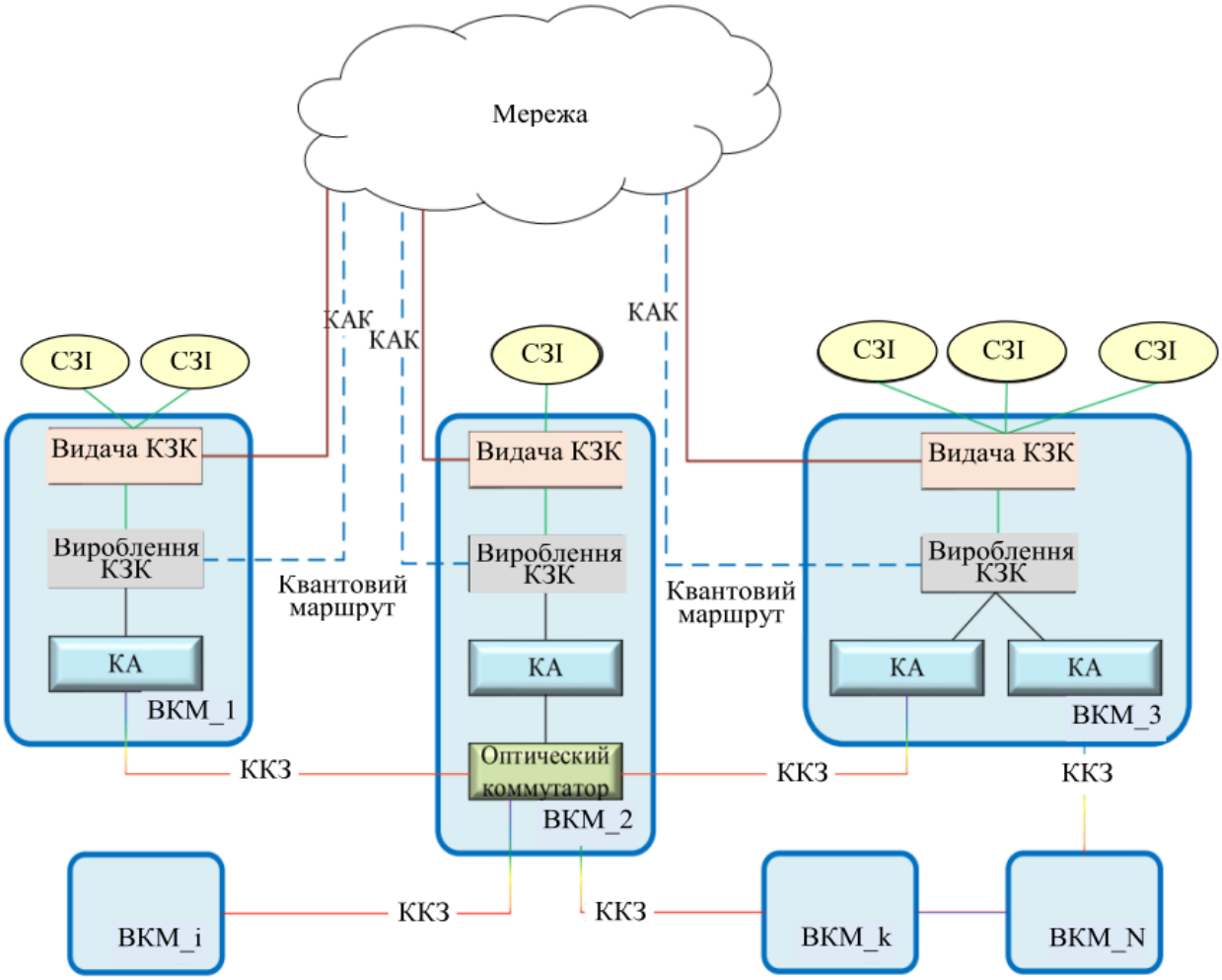

Рисунок 3.3 – Структура мережі КРК (по вузлах)

Рівень споживачів має такі функції:

- запит квантозахищеного ключа, можливо із зазначенням бажаних або необхідних параметрів запитуваного ключа;
- отримання квантозахищеного ключа відповідно до запиту;
- використання ключа згідно з призначенням у пристроях цього рівня.

Рівень керування КЗК повинен мати такі функції:

- організація сховищ квантозахищених ключів;
- синхронізація парних ключових сховищ (за наявності зв'язку);
- моніторинг запитів на квантозахищені ключі (прогнозування);
- обробка запитів квантозахищених ключів від зовнішніх систем захисту інформації (СЗІ);
- підтримання актуальної бази відповідності між СЗІ-споживачами та вузлами керування сеансом (ВКС), до яких вони підключені;
- формування запитів на КЗК до нижчого рівня генерації КЗК;
- отримання КЗК від рівня генерації КЗК;
- передавання КЗК СЗІ-споживачу.

Рівень генерації КЗК повинен мати такі функції:

- підтримання актуальної карти мережі;
- побудова оптимальних ланцюгів ВКС для формування КЗК;
- розподіл КЗК по визначених ланцюгах ВКС;
- організація сховищ квантових ключів;
- організація каналів, захищених квантовими ключами (для формування КЗК);
- побудова автентифікованого каналу для рівня генерації квантових ключів (за потреби);
- організація запитів на квантові ключі;
- отримання квантових ключів від рівня генерації квантових ключів;
- передавання квантозахищених ключів на рівень керування квантозахищеними ключами у відповідь на запит таких ключів.

Рівень генерації квантових ключів повинен мати такі функції:

- генерація квантових ключів;
- передавання квантових ключів на рівень генерації КЗК.

Таким чином, розроблено вимоги до трирівневої структури мережі КРК і функцій кожного рівня. Вищі рівні використовують результати роботи нижчих рівнів для свого функціонування. Згенеровані ключі зберігаються не на тому рівні, де вони були створені. Рівень генерації КЗК має менше навантаження порівняно з європейськими аналогами завдяки перенесенню частини функцій на рівень керування КЗК. При цьому допускається уніфікація всіх ВКС без виокремлення спеціальних типів (магістральних, доступових, користувацьких).

У разі необхідності підключення підмережі топології «зірка», тобто на основі спеціальних типів ВКС, підключення здійснюється центральним ВКС-сервером. При цьому порядок роботи підмережі не змінюється, а формування КЗК із деяким зовнішнім щодо підмережі ВКС здійснюється між зовнішнім ВКС і ВКС-сервером згідно із загальним порядком формування КЗК для мережі КРК змішаної топології. Сусідній ВКС мережі КРК змішаної топології, який не є ВКС-Клієнтом, не розглядається як периферійний вузол ВКС-Сервера для реалізації порядку функціонування підмережі топології «зірка».

3.5 Порядок розподілу КЗК у мережі КРК

Беручи до уваги всі раніше сформульовані вимоги до мережі КРК і її структури, можна визначити порядок роботи такої мережі під час створення квантозахищених ключів. Блок-схема процесу створення КЗК подана на рисунку 3.4. Кольори блоків відповідають кольору рівня мережі КРК, на якому здійснюється вказана дія. Для проведення першого сеансу КРК і запуску роботи мережі в цілому необхідне попереднє розподілення первинних ключів.

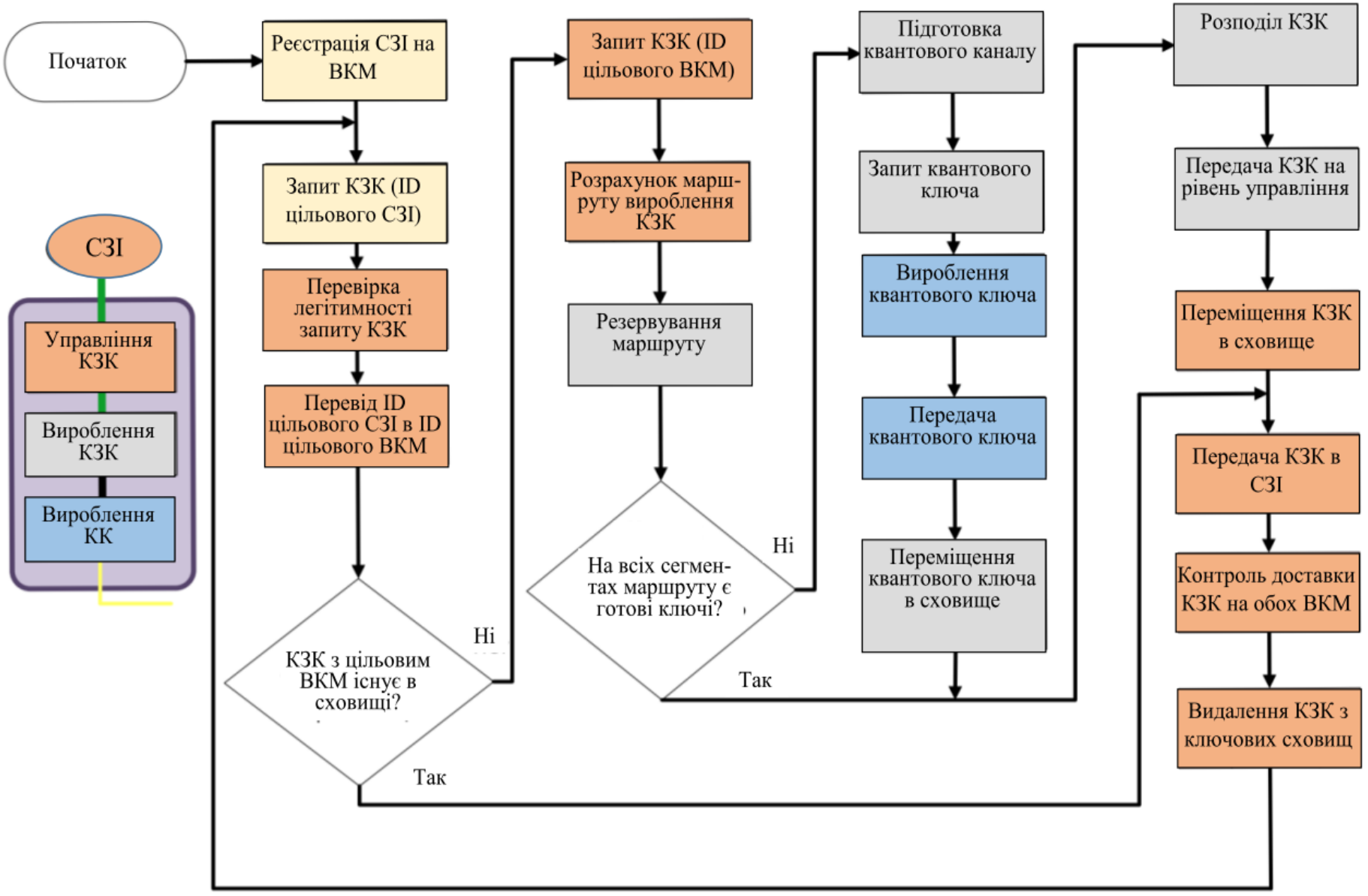

Рисунок 3.4 – Блок-схема процесу розподілу КЗК

3.6 Методика побудови мережі КРК змішаної топології

На основі розроблених раніше вимог до структури мережі та методики розподілу КЗК у мережі магістральної топології можна сформулювати методику побудови мережі КРК змішаної топології. Її графічне зображення в нотації IDEF0 наведено рисунку 3.5.

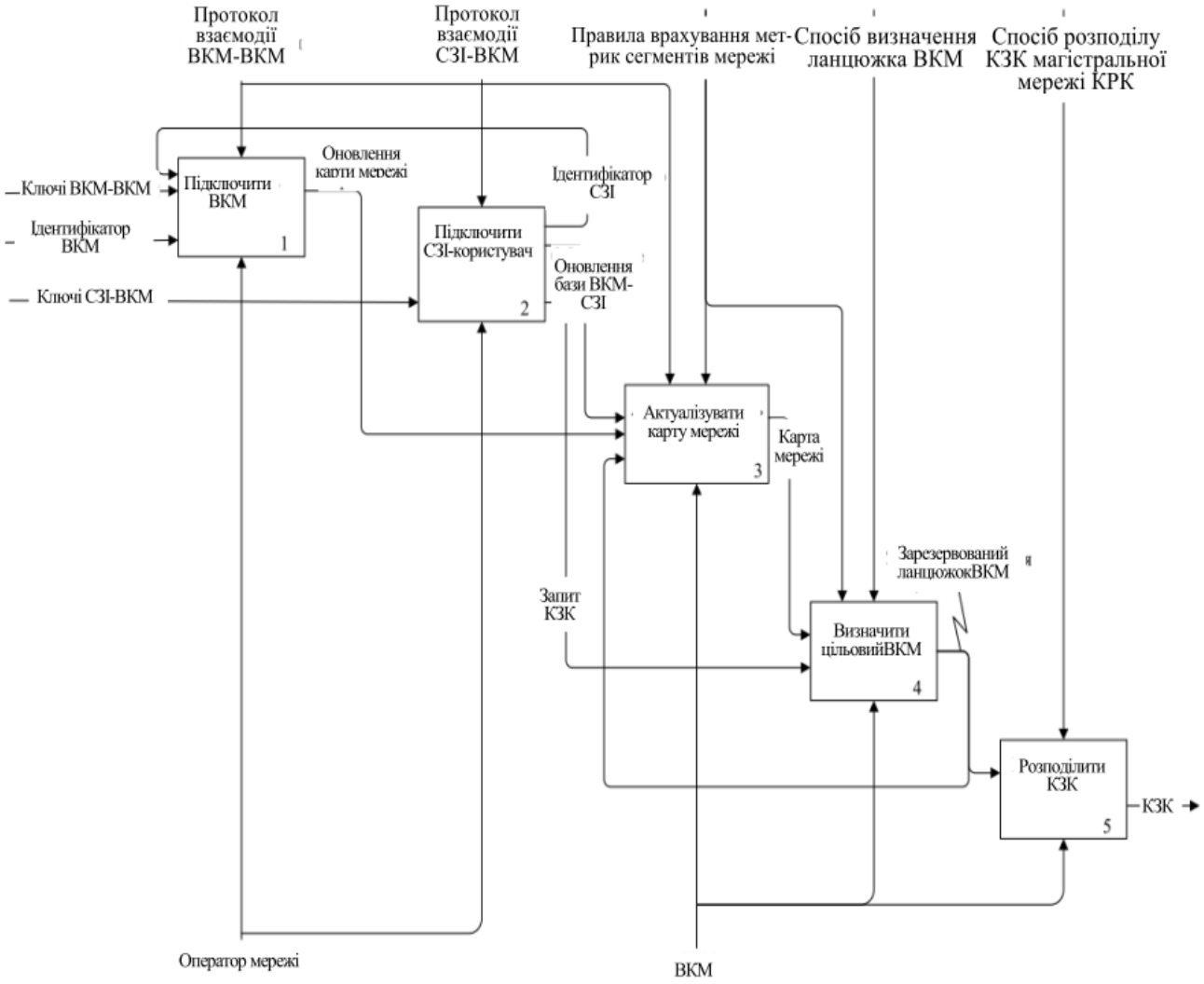

Рисунок 3.5 – Методика побудови мережі КРК

Мережа КРК будується з довірених вузлів, до кожного з яких можуть підключатися зовнішні користувацькі пристрої —СЗІ-споживачі. Кожен вузол мережі містить щонайменше один напівкомплект квантової апаратури та

з’єднаний квантовим каналом зв’язку щонайменше з одним сусіднім вузлом мережі. Граф з’єднань квантовими каналами мережі КРК має бути зв’язним.

Кожен вузол мережі КРК містить один або кілька модулів генерації квантових ключів, реалізованих за допомогою квантової апаратури. На поточний момент, через відсутність єдиного повністю стандартизованого протоколу КРК, на обох кінцях кожного квантового каналу має бути розміщена апаратура одного виробника, що працює за одним і тим самим протоколом КРК. На кожному сегменті мережі КРК можливе застосування різної квантової апаратури. Максимальна довжина квантового каналу кожного сегмента визначається граничними значеннями втрат у квантовому каналі, установленими для протоколу КРК, який використовується на цьому сегменті.

Для початку роботи мережі КРК, а саме — для запуску процесу генерації квантових ключів із подальшою можливістю розподілу КЗК, необхідно попередньо розподілити необхідні набори ключів, зокрема для автентифікації класичного каналу квантової апаратури між парами сусідніх ВКС, з’єднаних квантовим каналом.

Розрахунок магістральної підмережі виконується тим вузлом, на який надійшов запит на формування КЗК, на основі актуальної карти мережі КРК, що містить метрики сегментів мережі. Для визначення пар цільових ВКС, між якими необхідно розподілити КЗК згідно із запитом СЗІ-споживача, потрібно підтримувати актуальну базу відповідності між ВКС і підключеними до них СЗІ-споживачами для всієї мережі. При цьому ідентифікація всіх ВКС у мережі має бути унікальною, щоб забезпечити однозначне визначення цільових вузлів.

Мережа КРК може розбудовуватися поступово — ітераційно, шляхом підключення нових ВКС до вже існуючої мережі. Для підключення нового ВКС до діючої мережі КРК необхідно виконати такі умови:

– з’єднати новий ВКС із чинним квантовим каналом. Квантовий канал може бути підключений до вільного модуля генерації квантових ключів, що є в наявному ВКС; до оптичного комутатора, якщо ВКС підтримує

множинні квантові канали в одному модулі генерації; до нового модуля генерації квантових ключів, підключеного до існуючого ВКС для роботи з новим підключуваним вузлом;

– завантажити в чинний і новий ВКС попередньо розподілені ключі для побудови класичного автентифікованого каналу квантової апаратури в межах цієї пари ВКС. Попередньо розподілені ключі можуть бути створені за допомогою генератора випадкових чисел у складі ВКС із подальшою доставкою до нового ВКС довіреним кур’єром. Після успішного сеансу КРК із новим ВКС цей вузол вважається підключеним до мережі КРК;

– як класичні ключі захисту для розподілу КЗК між СЗІ-споживачами можуть використовуватися КЗК, розподілені з використанням захисту лише на квантових ключах у межах мережі КРК між новим ВКС і всіма необхідними цільовими ВКС.

ВИСНОВКИ

1. Здійснено аналіз сучасних технологій генерації ключів для криптографічних перетворень та відомих способів подолання максимальної дальності під час створення квантових ключів, що дозволило обгрунтувати опис вибраної технології та типової архітектури системи квантового розподілу ключів.

2. На основі аналіз структури мережі квантового розподілу ключів за версією ETSI розроблено алгоритм побудови автентифікованого каналу квантової апаратури та обгрунтовано варіанти використання хеш-функцій для автентифікації.

3. Згідно встановлених вимог до рівнів споживачів, генерації квантових ключів та формування квантовозахищених ключів розроблено алгоритм побудови мережі квантового розпоілу ключів.

4. Розроблено методику побудови та рекомендовану структуру мережі квантового розпоілу ключів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. К.: ДУТ, 2015. 449 с.
2. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія. Житомир: ЖНАЕУ, 2016. 636 с.
3. Лісовська Ю. Кібербезпека. Ризики та заходи. К.: Кондор, 2019. 272 с.
4. Schnorr C.P. Fast Factoring Integers by SVP Algorithms. Режим доступу: https://eprint.iacr.org/eprint-bin/getfile.pl?entry=2021/232&version=20210409: 151242&file=232.pdf.
5. ID Quantique SA. Quantum-safe Security. White Paper. Understanding Quantum Cryptography 2020. Режим доступу: https://marketing.idquantique.com/acton/attachment/11868/f-020d/1/-/-/-/-/Understanding%20Quantum%20Cryptography_White%20Paper.pdf.
6. Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Scientific and Statistical Computing. 1997. Vol. 26, No. 5. P. 1484–1509.
7. Quantum Safe Cryptography and Security. ETSI. Режим доступу: http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf
8. ID Quantique. Clavis300 Quantum Cryptography Platform Brochure. 2019. Режим доступу: https://marketing.idquantique.com/acton/attachment/11868/f-42e4a1b3-46a2-4f2f-8fcd-ba9118954c3a/1/-/-/-/-/Clavis300_QKD_Brochure.pdf.
9. Quantum Key Distribution Products. TOSHIBA CORPORATION. – Режим доступу: https://www.toshiba.co.jp/qkd/en/products.htm.
10. Bennet C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. Theoretical Computer Science. 2014. Vol. 560, pt.1. P. 175–179.

11. F.Laudenbach, C.Pacher, C.-H.F.Fung, A.Poppe, M.Peev, B.Schrenk, M.Hentschel, P.Walther, H.Hübel. Continuous-variable quantum key distribution with Gaussian modulation – the theory of practical implementations. Adv. Quantum Technol. 2018. Vol.1, No.1. P. 1870011

12. Garnerone S., Zanardi P., Lidar D.A. (2009). Adiabatic quantum computation in open systems. Physical Review Letters. 2009. Vol.102(11). P.110503.

13. A. Wonfor, C. White, A. Lord, R. Nejabati, T.P. Spiller, J.F. Dynes, A.J. Shields, R.V. Penty. Quantum networks in the UK. Proc. SPIE-11712, Metro and Data Center Optical Networks and Short-Reach Links IV. 2021. P. 1171207.

14. P. Chaiwongkhot, K.B. Kuntz, Y. Zhang, A. Huang, J.P. Bourgoin, S. Sajeed, N. Lutkenhaus, T. Jennewein. Eavesdropper's ability to attack a free-space quantum-key-distribution receiver in atmospheric turbulence. Phys. Rev. A. 2019. Vol. 99, No. 6. P. 062315.

15. V. Martin, A. Aguado, P. Salas, A.L. Sanz, J.P. Brito, D.R. Lopez, V. Lopez, A. Pastor, J. Folgueira, H.H. Brunner, S. Bettelli, F. Fung, L.C. Comandar, D. Wang, A. Poppe, M. Peev. The Madrid Quantum Network: A Quantum-Classical Integrated Infrastructure. Proceedings OSA Advanced Photonics Congress (AP)-2019 (IPR, Networks, NOMA, SPPCom, PVLED). 2019. P. QtW3E.5.

16. Y.A. Chen, Q. Zhang, T.Y. Chen, W.Q. Cai, S.K. Liao, J. Zhang, K. Chen, J. Yi, J.G. Ren, Z. Chen, S.L. Han. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature. 2021. Vol. 589. P. 214–219.

17. C. Elliot, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, H. Yeh. Current status of the DARPA quantum network. Proceedings of Quantum Information and Computation III. 2015. P. 8515.

18. Q. Zhang, F. Xu, Y.A. Chen, C.Z. Peng, J.W. Pan. Large scale quantum key distribution: challenges and solutions. Optics Express. 2018. Vol. 26. P. 24260.

19. L. Sheng-Kai, C. Wen-Qi, L. Wei-Yue, Z. Liang, L. Yang, R. Ji-Gang, Y. Juan, S. Qi, C. Yuan, L. Zheng-Ping, L. Feng-Zhi, C. Xia-Wei, S. Li-Hua, J. Jian-

Jun, W. Jin-Cai, J. Xiao-Jun, W. Jian-Feng, H. Yong-Mei, W. Qiang, Z. Yi-Lin, D. Lei, X. Tao, M. Lu, H. Tai, Z. Qiang, C. Yu-Ao, L. Nai-Le, W. Xiang-Bin, Z. Zhen-Cai, L. Chao-Yang, S. Rong, P. Cheng-Zhi, W. Jian-Yu, P. Jian-Weiю Satellite-to-ground quantum key distribution. Nature. 2017. Vol. 549. P. 43–47.

20. K. Günthner, I. Khan, D. Elser, B. Stiller, Ö. Bayraktar, C. Müller, K. Saucke, D. Tröndle, F. Heine, S. Seel, P. Greulich, H. Zech, B. Gütlich, S. Philipp-May, C. Marquardt, G. Leuchs. Quantum-limited measurements of optical signals from a geostationary satellite. Optica. 2017. Vol. 4, No. 6. P.611–616.

21. Сарапук О.І., Черняк В.А. Структура мережі квантового розподілу ключів за версією ETSI. Збірник матеріалів науково-практичного симпозіуму «Захист інформації’2025».Тернопіль, 2025. С.91-93.

22. Сарапук О.І., Рибінський В.О., Сапіташ В.І. Архітектура системи квантового розподілу ключів. Збірник матеріалів науково-практичної конференції моодих вчених, аспірантів та студентів «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ-2022). Тернопіль, 2025. С.111-113.

23. Scarani V., Acin A., Ribordy G., Gisin N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Physical Review Letters. 2004. Vol.92(5). P.057901.

24. Barker E. Recommendation for Key Management, Part 1: General. NIST. 2016. – Режим доступу: https://nvlpubs.nist.gov/nistpubs/ SpecialPublications/ NIST.SP.800-57pt1r4.pdf.

25. Mosca M. Cybersecurity in an era with quantum computers: will we be ready? IEEE Security & Privacy. 2018. Vol. 16, No. 5. P. 38–41.

26. Zhang Q., Xu F., Chen Y.A., Peng C.Z., Pan, J.W. Large scale quantum key distribution: Challenges and solutions. Optics Express. 2018. Vol.26(18). P.24260-24273.

27. Lucamarini M., Yuan Z., Dynes J F., Shields A.J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature. 2018. Vol.557(7705). P.400-403.

28. Korzh B., Lim C.W., Houlmann R., Gisin N., Li M.J., Nolan D., Zbinden, H. Provably secure and practical quantum key distribution over 307 km of optical fibre. Nature Photonics. 2015. Vol.9(3). P.163-168.

29. V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dusek, N. Lutkenhaus, M. Peev. The security of practical quantum key distribution. Reviews of Modern Physiscs. 2009. Vol. 81, No. 3. P. 1301.

30. Courtland R. China’s 2,000-km Quantum Link Is Almost Complete. IEEE spectrum. 2016. Vol. 53, No. 11. P. 11–12.

31. A. Wonfor, C. White, A. Bahrami, J. Pearse, G. Duan, A. Straw, T. Edwards, T. Spiller, R. Penty, A. Lord. Field trial of multi-node, coherent-one-way Quantum Key Distribution with encrypted 5×100G DWDM transmission system. 45th European Conference on Optical Communication (ECOC 2019). 2019. P. 1–4.

32. Industry Specification Group (ISG) on Quantum Key Distribution for users (QKD): ETSI. Режим доступу: https://www.etsi.org/committee/1430-qkd.

ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»
ГАЛИЦЬКИЙ ФАХОВИЙ КОЛЕДЖ ІМ. В'ЯЧЕСЛАВА ЧОРНОВОЛА

КІБЕРБЕЗПЕКА ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ (КБКІТ – 2025)

науково-практична конференція
молодих вчених, аспірантів та студентів

28–29 серпня 2025
Тернопіль

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

УДК 004.056.53

Сарапук О.І., Рибінський В.О., Сапіташ В.І.

Західноукраїнський національний університет

АРХІТЕКТУРА СИСТЕМИ КВАНТОВОГО РОЗПОДІЛУ КЛЮЧІВ

Вступ. Традиційні криптографічні методи, засновані на складності математичних задач, поступово втрачають надійність у зв'язку з появою потужних обчислювальних засобів і перспективних квантових обчислювачів, здатних ефективно зламувати класичні шифри. У цьому контексті особливої актуальності набувають квантові методи захисту інформації [1], зокрема квантовий розподіл ключів (КРК) (Quantum Key Distribution, QKD), який забезпечує безумовну стійкість криптографічного обміну завдяки використанню фундаментальних принципів квантової механіки [2].

Розробка ефективної архітектури системи квантового розподілу ключів є актуальним науково-технічним завданням і важливим кроком до впровадження квантової безпеки в практичні телекомунікаційні мережі, який визначає перспективи формування безпечних інформаційних середовищ у майбутніх квантових комунікаційних мережах.

Мета: розробити архітектуру системи квантового розподілу ключів.

1. Розробка архітектури системи квантового розподілу ключів

Квантова апаратура, що реалізує протокол КРК, являє собою комплекс із двох пристроїв, з'єднаних квантовим каналом. Спрощена архітектура комплексу наведена на рисунку 1.

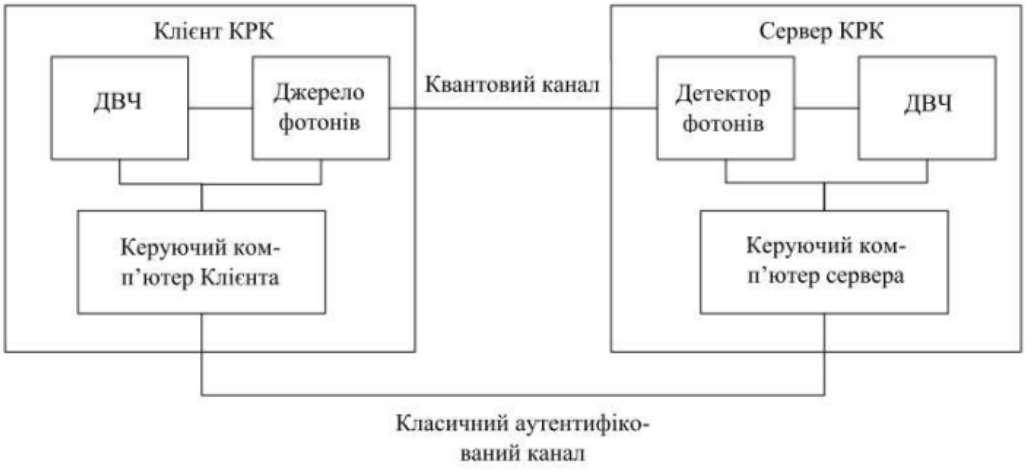

Рисунок 1 – Схема комплексу квантової апаратури

Один з пристроїв комплексу, що містить генератор (джерело) поодиноких фотонів, прийнято називати Клієнтом КРК. Суміжний пристрій, що містить детектор (приймач) поодиноких фотонів, називають Сервером КРК. Кожен з пристроїв має датчик випадкових чисел (ДВЧ). При цьому рекомендується використовувати датчики, в основі випадкових процесів яких лежать квантові ефекти, що дозволяє отримати істинно випадкову послідовність, з якої надалі формується квантовий ключ.

Сервер КРК і Клієнт КРК з'єднані двома логічними каналами: квантовим і класичним. Квантовий канал призначений для передачі квантових інформаційних станів, тобто фотонів і, як правило, реалізується за допомогою звичайного оптоволокна. Існують системи КРК, у яких як квантовий канал застосовується повітряне середовище, але вони поки що перебувають на стадії лабораторних установок.

Важливою особливістю технології КРК є повна доступність квантового каналу для зловмисника, тобто цей канал не контролюється і не захищається від втручання. Крім квантового каналу, Сервер і Клієнт КРК повинні бути з'єднані класичною лінією зв'язку, де реалізується класичний автентифікований канал. До цього каналу висуваються вимоги щодо забезпечення цілісності переданих даних та автентифікації відправника.

Реальна система КРК додатково має ще логічний службовий канал для передачі даних, який передає команди управління й моніторингу апаратури, не пов'язані безпосередньо з протоколом КРК. У деяких реалізаціях може знадобитися забезпечення не лише цілісності, а й конфіденційності цих даних. Для роботи системи КРК в апаратуру необхідно завантажити попередньо розподілені ключі, які потрібні щонайменше для побудови класичного автентифікованого каналу до першого успішного отримання достатньої кількості квантових ключів. Одну ітерацію реалізації протоколу КРК називають сеансом КРК.

Зазвичай кожен сеанс КРК складається з таких етапів:

– підготовка квантового каналу;
– передача поодиноких фотонів квантовим каналом;
– постобробка переданої послідовності.

У результаті передачі квантовим каналом обидва пристрої отримують так званий сирий ключ. Далі постобробка відбувається через класичний автентифікований канал і включає три підетапи:

– узгодження базисів вимірювання на стороні приймача з базисами кодування на стороні джерела. Неспівпадіння відкидаються, а сирий ключ перетворюється на просіяний ключ;

– виправлення помилок у просіяних ключах для отримання ідентичних послідовностей у Сервері та Клієнті КРК. Результат – очищений ключ;

– посилення секретності – стиснення очищеного ключа для зменшення інформації, доступної зловмиснику. Результат – секретний квантовий ключ.

На рисунку 2 представлена узагальнена послідовність виконання протоколу КРК.

Потрібно відзначити, що результат роботи квантового протоколу не зовсім коректно називати квантовим ключем. Правильніше говорити, що результатом сеансу КРК є випадкова квантова ґамма, ідентична у двох абонентів, оскільки цей результат має змінну довжину, яка не завжди збігається з довжиною ключів, що застосовуються в алгоритмах кодування. Більше того, результат виконання одного й того ж протоколу КРК суттєво відрізняється для квантових каналів із низькими та високими втратами, що безпосередньо впливають на величину помилок під час передачі в квантовому каналі (QBER). Це, своєю чергою, впливає на обсяг

інформації про квантову ґамму, доступної порушнику, і яка зменшується на етапі посилення секретності.

Рисунок 2 – Послідовність виконання протоколу КРК

Згідно з експериментальними даними, наведеними у [1], при довжині лінії у 50 км (що відповідає втратам 10 дБ при типовому затуханні у ВОЛЗ 0,2 дБ/км [2]) ефективність вироблення квантових ключів, тобто відношення числа зареєстрованих імпульсів на сервері КРК до загальної кількості імпульсів, відправлених клієнтом КРК, становить 2×10^{-5}. Таким чином, щоб отримати 256-бітний квантовий ключ при довжині лінії 50 км за один сеанс КРК, потрібна послідовність у 2×10^{7} імпульсів. Втрати при довжині квантового каналу у 100 км складають 20 дБ, тобто у 10 разів більше, ніж при 50 км. Тому для вироблення 256-бітного квантового ключа за один сеанс КРК послідовність імпульсів, що передається квантовим каналом, має бути в 10 разів більшою, тобто не менше, ніж 2×10^{8} імпульсів.

Висновок. Розроблено архітектуру системи квантового розподілу ключів, що дало можливість регулярної генерації спільних квантових ключів у користувацькі пристрої.

Перелік використаних джерел.

1. Quantum Safe Cryptography and Security [Електронний ресурс]. ETSI. Режим доступу: http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.

2. Quantum Key Distribution Products [Електронний ресурс]. TOSHIBA CORPORATION. Режим доступу: https://www.toshiba.co.jp/qkd/en/products.htm.




ЗАХІДНОУКРАЇНСЬКИЙНАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КІБЕРБЕЗПЕКИ
ГРОМАДСЬКА ОРГАНІАЦІЯ «КІБЕРБЕЗПЕКА І АВТОМАТИЗАЦІЯ»

Матеріали
науково-практичного симпозіуму

"ЗАХИСТ'ІНФОРМАЦІЇ'2025"

28 листопада 2025
Тернопіль

УДК 004.056.53

***Сарапук О.І.*[1]*, Черняк В.А.*[2]**

[1]*Західноукраїнський національний університет*

[2] *Відокремлений структурний підрозділ «Рівненський фаховий коледж Національного університету біоресурсів і природокористування України»*

СТРУКТУРА МЕРЕЖІ КВАНТОВОГО РОЗПОДІЛУ КЛЮЧІВ ЗА ВЕРСІЄЮ ETSI

Вступ. Розробка уніфікованої структури мережі квантового розподілу ключів (КРК) за специфікаціями ETSI [1] є надзвичайно актуальною через швидке наближення практичної загрози з боку квантових комп'ютерів — вже зараз зростає ризик «збирання сьогоднішніх зашифрованих даних для розшифровки пізніше». Стандартизована архітектура дозволяє трансформувати поодинокі пілотні лінії досліджень у масштабовані, сумісні між виробниками мережі та додатками рішення.

ETSI як галузева ініціатива вже оприлюднила набір документів, що визначають ролі вузлів, інтерфейси, протоколи доставки ключів та захисні профілі (наприклад, GS QKD 015 – архітектура, GS QKD 014 – REST-API доставки ключів, GS QKD 016 – захисний профіль). Використання цих специфікацій забезпечує інтероперабельність обладнання від різних постачальників, стандартизовані інтерфейси для оркестрації та управління ключовими ресурсами, а також підґрунтя для сертифікації та оцінки безпеки.

Мета: проаналізувати структуру мережі КРК за версією ETSI.

1. Структура мережі квантового розподілу ключів

Група стандартизації ETSI у сфері квантового розподілу ключів охоплює різні сфери застосування КРК: безпеку протоколів і реалізацій КРК, інтерфейси взаємодії, методи вимірювань тощо. Перший варіант мережі КРК був представлений у описі інтерфейсу взаємодії квантової апаратури та СЗІ.

Мережа КРК побудована з довірених вузлів (рисунок 1).

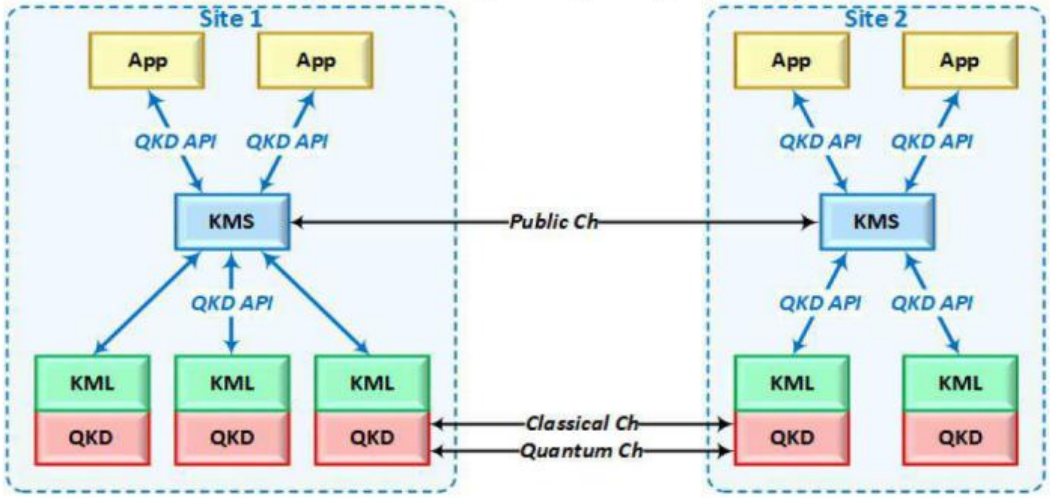

Рисунок 1 – Структура мережі КРК за документом ETSI GS QKD 004

У сценарії взаємодії відповідно до ETSI GS QKD 004 беруть участь; апаратне забезпечення КРК – QKD; сервер управління квантовими ключами – KML; сервер управління ключами – KMS; клієнти мережі, користувацькі застосунки – App.

Система побудована з незалежних частин. Довірений вузол містить кілька екземплярів квантової апаратури, сервери управління квантовими ключами, сервер управління ключами. При цьому до довіреного вузла включається також користувацький застосунок, для якого генеруються секретні ключі. Далі проводиться аналіз кожного з об'єктів довіреного вузла та його функцій.

Базовим елементом мережі КРК є квантова апаратура. При цьому сполучені пари комплектів квантової апаратури, з'єднані як квантовим, так і класичним автентифікованим каналом, є самодостатнім елементом. Генерація квантових ключів відбувається незалежно від інших процесів у мережі КРК.

Квантова апаратура генерує не ключ, а випадкову послідовність нефіксованої довжини. Для формування квантових ключів із сукупності випадкових послідовностей застосовуються сервери управління квантовими ключами (KML). На кожен блок квантової апаратури в кожному вузлі комутації мережі (ВКМ) припадає по одному серверу управління квантовими ключами. Ця частина ВКМ формує квантові ключі з послідовностей, отриманих від квантової апаратури, зокрема присвоюючи ідентифікатори квантових ключів та іншу метаінформацію. Сервер управління містить сховище квантових ключів, у яке поміщаються сформовані квантові ключі з усією необхідною метаінформацією. При цьому їх ідентичність ґрунтується лише на довірі до протоколу КРК, що теоретично гарантує ідентичність сформованих послідовностей.

Для передавання спільних секретів у СЗІ-споживачі, закріплені за ВКМ, не з'єднаними безпосередньо квантовим каналом, використовується сервер управління ключами (KMS). Цей елемент ВКМ у ранніх документах ETSI описаний поверхнево, без зазначення способу розподілу спільного секрету між несусідніми вузлами. Як захист передавання квантового ключа використовується кодування одноразовим блокнотом.

Таким чином, перший варіант мережі КРК за версією ETSI являє собою чотирирівневу структуру. Два рівні мережі оперують квантовими ключами, третій рівень призначений для передавання квантових ключів, згенерованих на одному сегменті мережі КРК, на інші сегменти. Четвертий рівень мережі – рівень користувацьких застосунків. Другий рівень мережі досить чисельний за кількістю елементів, кожен з яких виконує лише невелику частину функцій, реалізованих у ВКМ, і може бути оптимізований. Третій рівень, навпаки, є найбільш навантаженим елементом ВКМ.

Пізніше був випущений стандарт ETSI GS QKD 014 V1.1.1, у якому внесено суттєві зміни до опису структури мережі КРК, схематичне зображення якої наведено на рисунку 2. У сценарії роботи беруть участь: апаратне забезпечення КРК – QKDE; сутність управління ключами – KME; клієнти мережі – SAE. Видно, що відбулося суттєве спрощення структури мережі шляхом об'єднання сервера управління квантовими ключами та сервера управління ключами в єдиний об'єкт.

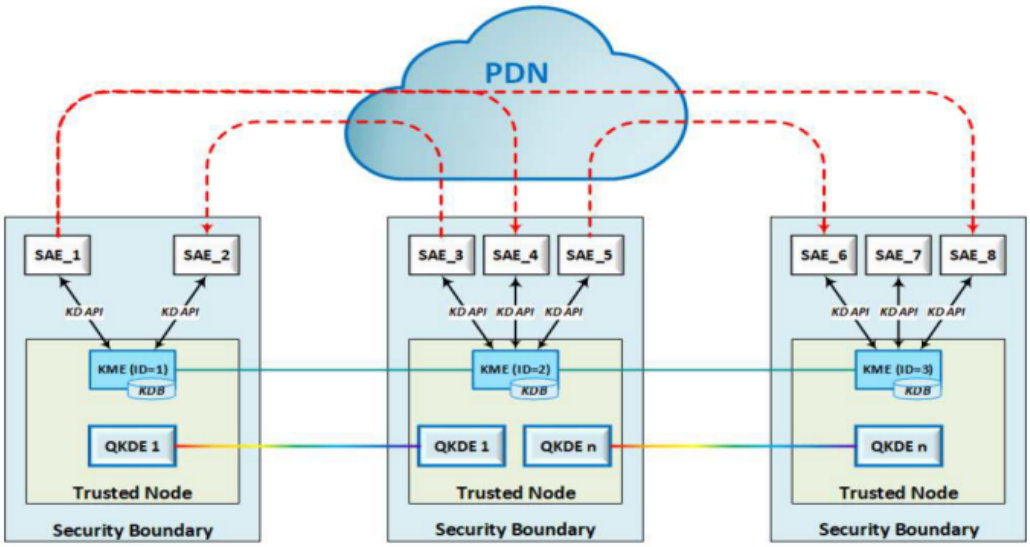

Рисунок 2 – Структура мережі КРК згідно з ETSI GS QKD 014

При цьому інтерфейс взаємодії описується з таких припущень: вузол працює та управляється безпечно; KME і SAE перебувають у межах одного вузла; інтерфейс взаємодії не виходить за межі контрольованої зони довіреного вузла; KME є безпечним; SAE є безпечним; KME має мати унікальний ідентифікатор у межах мережі КРК; SAE має мати унікальний ідентифікатор у межах мережі КРК.

Таким чином, початкова структура мережі містила чотири рівні, розділяючи управління квантовими ключами та формування спільних секретів згідно з запитами користувачів застосунків. При цьому користувацькі застосунки включалися до складу довірених вузлів мережі, що не зовсім коректно. У наступній версії структури мережі цей недолік був виправлений: користувацькі застосунки були винесені за межі мережі,. Водночас спрощення структури вузла шляхом об'єднання блоків управління квантовими ключами та взаємодії з користувацькими застосунками ускладнює вузол мережі, оскільки майже всі функції вузла концентруються в єдиному блоці.

В обох версіях мережі КРК не розглядаються способи розподілу спільного секрету для користувацьких застосунків, питання захисту каналів взаємодії вузлів та управління вузлами мережі. Для другої версії мережі КРК додані абстрактні вимоги щодо безпеки вузлів мережі, які не сприяють спрощенню побудови мережі КРК загалом і довірених вузлів зокрема.

Висновок. Детально проаналізовано структуру мережі КРК за версією ETSI, що дало можливість обгрунтувати вибір структури згідно конкретної задачі.

Перелік використаних джерел.

1. ETSI GS QKD 004 v.2.1.1 Quantum Key Distribution (QKD); Application Interface. Режим доступу: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/02.01.01_60/gs_QKD004v020101p.pdf.

2. ETSI GS QKD 014 V1.1.1 Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API.2019. Режим доступ: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_QKD014v010101p.pdf.