НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ І ГЛОБАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ

Кваліфікаційна наукова
праця на правах рукопису

Зінченко Володимир Леонідович

УДК 004.043

ДИСЕРТАЦІЯ

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ КОНТРОЛЮ ТА КЛАСИФІКАЦІЇ СТАНІВ В ОПТИЧНИХ ЛІНІЯХ ПЕРЕДАЧІ ДАНИХ

122 – «Комп’ютерні науки»

Галузь знань 12 – Інформаційні технології

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

В.Л. Зінченко

Науковий керівник:
Лифар Володимир Олексійович
доктор технічних наук

Київ – 2025

АНОТАЦІЯ

Зінченко В.Л. «Інформаційна технологія контролю та класифікації станів в оптичних лініях передачі даних». Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки» – Інститут телекомунікацій і глобального інформаційного простору Національна академія наук України, Київ, 2025.

Дисертація спрямована на розробку моделей та методів інформаційної технології для визначення аномальних станів у оптичних лініях зв'язку з метою забезпечення прийнятної надійності процесу передачі даних.

У вступі розкрита актуальність дослідження безпеки оптичних каналів зв'язку, визначено об'єкт, предмет, мету та завдання роботи. Сформульовано наукову новизну й практичне значення результатів, які спрямовані на створення інформаційної технології для визначення типів аномалій та штатних режимів за для підвищення надійності виконання функцій передачі даних.

У першому розділі проведено теоретичний аналіз проблем безпеки квантових каналів зв'язку. На основі аналізу джерел інформації за темою дослідження показано, що, попри стрімкого розвитку протоколів квантового розподілу ключів залишається низка невирішених питань по захисту інформації. Відомі атаки на практичні системи, зокрема розділення числа фотонів, засліплення детектора, та троянський кінь, доводять, що навіть квантові системи не є повністю захищеними. Це змушує замислитися над тим, наскільки ефективними є наявні підходи по забезпеченню захищеності, чи здатні вони виявляти приховані загрози в реальних умовах експлуатації і реагувати на відповідні загрози.

Особлива увага приділяється питанням ефективного моніторингу параметрів квантового каналу та виявлення аномалій. З одного боку, традиційні статистичні методи дають змогу оцінювати середні характеристики, проте їхня чутливість обмежена. З іншого боку, зростає інтерес до методів кластерного аналізу та

машинного навчання, які можуть розкрити закономірності, недоступні класичним підходам.

У другому розділі роботи представлено математичну та імітаційну моделі інформаційної технології аналізу стану каналу передачі даних та функціональну схему контролю станів каналу інформації на основі нейронної мережі. Вихідною точкою є загальні положення та концептуальна постанова задачі, що полягає у створенні методу імітаційного динамічного моделювання подій в віртуальному каналі зв'язку. Такий підхід дає змогу формалізувати причинно-наслідкові зв'язки між подіями та станами фотонів, а також досліджувати вплив квантових ефектів і атак на роботу системи. Використання цього підходу уможливлює побудову більш гнучких і точних механізмів моніторингу, що є основою для подальшої оптимізації систем безпечного зв'язку.

У межах розділу сформовано методи інтелектуального аналізу станів квантового каналу, які враховують ознаки когерентних та некогерентних атак, ефект спостерігача, принцип неможливості клонування та властивості квантової заплутаності. Ці методи дозволяють описувати поведінку параметрів каналу як сукупність підсистем, кожна з яких може перебувати у працездатному або у стані відмови. Для цього застосовуються методи класифікації та кластеризації, які інтегруються в архітектуру та модель нейронної мережі.

У розділі розроблено математичну модель оцінки відмов та критичних станів каналу, яка представлена у вигляді кортежу множин параметрів (графу), регістрів та функцій переходу. Ця модель описує динаміку роботи каналу, враховуючи детерміновані та стохастичні процеси. Модель інтегрує класичні принципи теорії кодування з особливостями квантових систем, зокрема неможливістю клонування квантових станів.

Завершальним етапом є побудова імітаційної моделі контролю квантового каналу та функціональної схеми інтелектуального аналізу, реалізованої на основі багатошарової нейронної мережі. Запропоновано архітектуру з вхідним шаром симптомів, проміжним шаром патерів і синдрому з вихідним шаром рішень. Така

структура дозволяє відобразити причинно-наслідкові зв’язки між параметрами каналу і можливими відмовами, забезпечуючи ефективну класифікацію станів. Це створює основу для розробки програмного забезпечення, яке здатне працювати в режимі OLAP, здійснювати діагностику каналу в реальному часі та вибрати дії для підвищення надійності й безпеки квантових систем передачі даних.

У третьому розділі проведено систематичний розгляд методів статистичного та інтелектуального аналізу даних, які інтегруються в інформаційну технологію для класифікації режиму роботи каналу передачі інформації. Вихідним пунктом є усвідомлення того, що навіть у квантових комунікаціях, де застосовуються фундаментальні принципи квантової механіки, безпека каналу не є абсолютною. Канал зв’язку може піддаватися як природним стохастичним флуктуаціям, так і цілеспрямованим атакам, що проявляються через зміну фізичних параметрів сигналу. Це зумовлює потребу в методах аналізу, здатних своєчасно виявляти такі відхилення та формувати рішення щодо стану системи.

Первинним рівнем обробки даних є статистичний аналіз. Він забезпечує формальне описання розподілів параметрів каналу, які інтерпретуються як багатовимірні дані з часовими залежностями. Обчислення середніх значень, стандартних відхилень, коефіцієнтів варіації дає змогу оцінити базову стабільність системи та порівняти різні режими роботи. Впровадження показника Z-score переводить усі параметри в єдину нормовану шкалу та дозволяє автоматично ідентифікувати відхилення. Така уніфікація ознак є необхідною умовою для подальшого застосування алгоритмів машинного навчання.

За допомогою коефіцієнта Пірсона досліджуються кореляційні зв’язки між параметрами. В результаті у стаціонарному режимі зв’язки майже відсутні, але стають суттєвими в умовах аномального режиму роботи каналу. Візуалізація у вигляді теплових карт і гістограм дозволяє ідентифікувати латентні закономірності, асиметрії чи мультимодальні розподіли. Таким чином, статистичний аналіз не обмежується лише числовими оцінками, а трансформується у базу для побудови інтелектуальних алгоритмів.

У цьому розділі також представлено інтелектуальні методи кластеризації та машинного навчання. Алгоритм k-means застосовується для групування даних результатів спостережень без попередньо заданих міток. Це дозволяє виявляти приховані стани каналу та автоматично відокремлювати стаціонарний режим від аномального. Застосування багатошарового перцептрона (MLP) є логічним продовженням статистичних і кластерних методів, оскільки надає змогу реалізувати класифікацію станів каналу в реальному часі з необхідною точністю та стійкістю до шумів.

У четвертому розділі здійснено розробку імітаційних моделей та віртуальний канал передачі даних для виконання процедур з застосуванням інтелектуальних методів машинного навчання. Якщо статистичні підходи дозволяють описати поведінку параметрів каналу, то нейронні мережі здатні виявляти приховані нелінійні залежності та своєчасно фіксувати критичні відхилення. Такий перехід є закономірним кроком у розвитку інформаційних технологій для підвищення надійності каналів комунікацій.

Підготовка даних розглядається як фундаментальний етап: часові вимірювання трансформуються у вектори статистичних ознак, що робить їх придатними для навчання моделей.

Вибір багатошарової нейронної мережі обґрунтовано її здатністю апроксимувати складні відображення у багатовимірному просторі ознак. Це рішення виводить систему за межі аналізу і переводить її в площину інтелектуальної діагностики, де модель не лише спостерігає, а й робить узагальнені висновки про стан каналу.

Оцінка моделі базується на комплексі метрик (accuracy, precision, recall, F1), що дає змогу досягти балансу між чутливістю до аномалій і стійкістю до хибних спрацьовувань. Таким чином, питання класифікації набуває характеру оптимізації ризиків.

Завершальною ланкою є інтеграція моделі в структурно-функціональну схему квантового каналу, де локальні прогнози об’єднуються у глобальне рішення. Це

демонструє практичну цінність поєднання статистичних та інтелектуальних методів, що формує основу нової інформаційної технології для квантових комунікацій.

Ключові слова: протокол BB84; канал зв’язку; статистичний аналіз; кластерний аналіз; нейронна мережа; аномалії; інформаційна технологія підтримки рішень.

ANNOTATION

Zinchenko V. L. “Information Technology for Monitoring and Classification of States in Optical Data Transmission Lines.” Qualification scientific work (manuscript). Dissertation submitted for the degree of Doctor of Philosophy in specialty 122 “Computer Science” - Institute of Telecommunications and Global Information Space, National Academy of Sciences of Ukraine, Kyiv, 2025.

The dissertation is focused on the development of models and methods of information technology for detecting anomalous states in optical communication lines in order to ensure acceptable reliability of the data transmission process.

The Introduction reveals the relevance of research on the security of optical communication channels, and defines the object, subject, aim, and objectives of the study. The scientific novelty and practical significance of the results are formulated, directed toward the creation of an information technology for identifying types of anomalies and normal operating modes with the purpose of enhancing the reliability of data transmission functions.

The first chapter provides a theoretical analysis of the security challenges inherent in quantum communication channels. A comprehensive review of scholarly and technical sources demonstrates that, despite the rapid advancement of Quantum Key Distribution (QKD) protocols, a number of unresolved issues concerning information protection persist. Documented attacks on practical implementations - in particular, Photon Number Splitting (PNS), Detector Blinding, and Trojan-Horse strategies - confirm that quantum systems cannot be regarded as entirely secure. These findings raise critical questions about the actual effectiveness of existing security mechanisms and emphasize the need to assess their ability to detect concealed threats under real operating conditions and to provide timely countermeasures.

Special attention is devoted to the problem of effective monitoring of quantum channel parameters and the detection of anomalies. While traditional statistical methods

allow for the estimation of average characteristics, their sensitivity is inherently limited. By contrast, the growing interest in clustering techniques and machine learning approaches reflects their potential to uncover complex patterns and dependencies that remain inaccessible to classical analytical methods.

The second chapter presents the mathematical and simulation models of the information technology designed for analyzing the state of the data transmission channel, as well as the functional scheme for monitoring the states of the information channel based on a neural network. The starting point is the general provisions and the conceptual formulation of the task, which consists in the development of a method for simulation-based dynamic modeling of events in a virtual communication channel. This approach makes it possible to formalize cause-and-effect relationships between events and photon states, as well as to investigate the influence of quantum effects and adversarial attacks on system performance. Employing this approach enables the construction of more flexible and accurate monitoring mechanisms, which constitute the foundation for further optimization of secure communication systems.

Within this chapter, methods of intelligent analysis of quantum channel states are developed, taking into account the characteristics of coherent and incoherent attacks, the observer effect, the no-cloning theorem, and the properties of quantum entanglement. These methods allow for the representation of channel parameter behavior as a collection of subsystems, each of which may operate either in a functional state or in a state of failure. To this end, classification and clustering techniques are applied and integrated into the architecture and model of the neural network.

A mathematical model for assessing channel failures and critical states has been developed, represented in the form of a tuple of parameter sets (graph), registers, and transition functions. This model describes the channel’s operational dynamics while incorporating both deterministic and stochastic processes. It integrates classical principles of coding theory with the specific features of quantum systems, in particular the impossibility of cloning quantum states.

The final stage involves the construction of a simulation model for quantum channel monitoring and a functional scheme of intelligent analysis implemented on the basis of a multilayer neural network. The proposed architecture consists of an input layer of symptoms, an intermediate layer of patterns and syndromes, and an output layer of decisions. Such a structure makes it possible to represent the causal relationships between channel parameters and potential failures, thereby ensuring effective state classification. This, in turn, establishes the groundwork for the development of software capable of operating in OLAP mode, performing real-time channel diagnostics, and selecting corrective actions to enhance the reliability and security of quantum data transmission systems.

The third chapter provides a systematic examination of statistical and intelligent data analysis methods that are integrated into the information technology framework for classifying the operating mode of the data transmission channel. The starting point is the recognition that even in quantum communications, where the fundamental principles of quantum mechanics are applied, channel security is not absolute. A communication channel may be subject both to natural stochastic fluctuations and to deliberate attacks manifested through variations in the physical parameters of the signal. This necessitates the development of analytical methods capable of promptly detecting such deviations and formulating decisions regarding the state of the system.

The primary level of data processing is statistical analysis. It provides a formal description of parameter distributions in the channel, which are interpreted as multidimensional data with temporal dependencies. The calculation of means, standard deviations, and coefficients of variation makes it possible to assess the baseline stability of the system and to compare different operating regimes. The introduction of the Z-score metric converts all parameters into a unified normalized scale, thereby enabling the automatic identification of anomalies. Such unification of features is a necessary prerequisite for the subsequent application of machine learning algorithms.

Pearson’s correlation coefficient is employed to study interdependencies among parameters. As a result, correlations are found to be negligible under stationary conditions, yet they become significant in anomalous channel states. Visualization in the form of

heatmaps and histograms enables the identification of latent patterns, asymmetries, or multimodal distributions. Thus, statistical analysis extends beyond numerical assessments and evolves into a foundation for constructing intelligent algorithms.

This chapter also introduces intelligent methods of clustering and machine learning. The k-means algorithm is employed to group observational data without predefined labels, thereby enabling the detection of hidden channel states and the automatic separation of stationary from anomalous regimes. The application of a Multilayer Perceptron (MLP) constitutes a logical continuation of statistical and clustering approaches, as it provides the capability to perform real-time classification of channel states with the required accuracy and robustness to noise.

The fourth chapter presents the development of simulation models and a virtual data transmission channel for implementing procedures based on intelligent machine learning methods. Whereas statistical approaches make it possible to describe the behavior of channel parameters, neural networks are capable of detecting hidden nonlinear dependencies and promptly capturing critical deviations. Such a transition represents a logical step in the evolution of information technologies aimed at enhancing the reliability of communication channels.

Data preparation is considered a fundamental stage: temporal measurements are transformed into vectors of statistical features, thereby making them suitable for model training.

The choice of a Multilayer Perceptron (MLP) is justified by its ability to approximate complex mappings in a multidimensional feature space. This decision extends the system beyond conventional analysis and places it within the domain of intelligent diagnostics, where the model not only observes but also produces generalized conclusions regarding the state of the channel.

Model evaluation is based on a set of metrics (accuracy, precision, recall, F1), which ensures a balance between sensitivity to anomalies and robustness against false positives. In this way, the task of classification acquires the characteristics of risk optimization.

The final stage is the integration of the model into the structural-functional scheme of the quantum channel, where local predictions are aggregated into a global decision. This demonstrates the practical value of combining statistical and intelligent methods, which together form the foundation of a novel information technology for quantum communications.

Keywords: BB84 protocol; communication channel; statistical analysis; cluster analysis; neural network; anomalies; decision support information technology.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації

Публікації у фахових виданнях:

1) Зінченко, В. Л., & Лифар, В. О. (2024). Інтелектуальний аналіз інформаційних потоків у квантових системах передачі інформації. International Scientific Technical Journal "Problems of Control and Informatics," 69(1), 80–86. https://doi.org/10.34229/1028-0979-2024-1-7 **(кат. А)**

2) Зінченко, В. Л., & Лифар, В. О. (2024). Інформаційна та математична модель процесів контролю стану квантового каналу зв'язку. Екологічна безпека та природокористування, 51(3), 151–160. https://doi.org/10.32347/2411-4049.2024.3.151-160 **(кат. Б)**

Публікації у виданнях, що входять до міжнародних науково-метричних баз:

3) Lyfar, V., Lyfar, O., & Zynchenko, V. (2024). METHODS OF INTELLIGENT DATA ANALYSIS USING NEURAL NETWORKS IN DIAGNOSIS. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 14(2), 109–112. https://doi.org/10.35784/iapgos.5746 (Scopus) ISSN 2391-6761

DOI: https://doi.org/10.35784/iapgos.5746 p-ISSN 2083-0157, e-ISSN 2391-6761

https://ph.pollub.pl/index.php/iapgos/article/view/5746/4583

https://www.scopus.com/authid/detail.uri?authorId=59216854100

Наукові праці, які засвідчують апробацію матеріалів дисертації:

4) Зінченко, В. Л., & Лифар, В. О. (2024, жовтня). Використання нейронних мереж для оптимізації квантових каналів зв'язку у квантовій криптографії. У Матеріали науково-практичної конференції з інформаційних технологій (м. Миколаїв, Україна). Інформаційні технології: моделі, алгоритми, системи (ITMAS – 2024). С 102-103.

5) Зінченко, В. Л., & Захожай, О. І. (2025, 26 березня). Інформаційна модель виявлення та класифікації атак у квантових каналах зв’язку на основі кластерного аналізу [Тези доповіді]. Innovative Approaches in Modern Science and Technology (Lisbon, Portugal). С. 116–117.

6) Захожай О.І., Зінченко В.Л. Телекомунікаційні засоби віддаленого доступу до робочих станцій. IX Всеукраїнська науково-практична конференція «Електроніка та телекомунікації: матеріали IX Всеукр.науково-практ.конф., м.Сєвєродонецьк. / М-во освіти і науки України, Східноукр. Нац. Ун-т ім.Даля; редкол.: Поркуян О.В. (та ін.) – Сєвєродонецьк: Східноукр.нац.ун-т ім. В.Даля, 2019 – 183 с. С.75-78.

7) Захожай О.І., Концевода О.А., Зінченко В.Л. Авторизація пристроїв IOT за допомогою MAC-адресу. X Всеукраїнська науково-практична конференція «Електроніка та телекомунікації: матеріали X Всеукр.науково-практ.конф., м.Сєвєродонецьк. / М-во освіти і науки України, Східноукр. Нац. Ун-т ім.Даля; редкол.: Поркуян О.В. (та ін.) – Сєвєродонецьк: Східноукр.нац.ун-т ім. В.Даля, 2020 – 127 с.

8) Кряжич О.О., Захожай О.І., Зінченко В.Л., Лифар В.О., Іванов В.Г. Підхід до реалізації веб-сервісу обробки інформації у графічних форматах. Сучасні інформаційні технології управління екологічною безпекою, природокористуванням, заходами в надзвичайних ситуаціях: виклики 2021 року. Колективна монографія за матеріалами XX Міжнародної науково-практичної конференції (Київ, 4-8 жовтня 2021 р.) / За заг. ред. С.О. Довгого. - К.: ТОВ «Видавництво «Юстон», 2021. с. 154-158. ISBN 978-617-7854-58-5. 1_zbirka_2021.pdf (itgip.org).

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

QBER - Quantum Bit Error Rate;

PNS - photon-number-splitting;

MDI-QKD - measurement-device-independent;

CV-QKD - continuous-variable QKD;

PNS - photon-Number Splitting;

PM-QKD - phase-Matching QKD;

TF-QKD - twin-Field QKD;

OLAP - Online Analytical Processing;

ІТ – інформаційні технології;

ІТППР - інформаційна технологія підтримки прийняття рішень;

СППР - система підтримки прийняття рішень;

ККЗ - квантовий канал зв’язку;

ІДМ - імітаційна динамічна модель;

ВСТУП

Актуальність теми дисертаційного дослідження. Стрімкий розвиток цифрових технологій та зростання обсягів даних у глобальних інформаційних системах зумовлюють підвищені вимоги до рівня безпеки передавання критично важливої інформації. Традиційні криптографічні методи, що ґрунтуються на складності математичних обчислень, поступово втрачають ефективність у зв’язку з появою високопродуктивних обчислювальних засобів, включно з квантовими комп’ютерами. Це створює загрозу компрометації класичних криптографічних протоколів у середньо- та довгостроковій перспективі.

Одним із перспективних напрямів забезпечення захищеного обміну даними є квантова передача інформації, яка базується на фундаментальних законах квантової механіки. Використання таких протоколів, як BB84, B92 та їхніх модифікацій, дозволяє гарантувати виявлення будь-якого несанкціонованого втручання в канал зв’язку. Водночас практична реалізація квантових каналів супроводжується низкою викликів: впливом фізичних обмежень оптичного середовища, шумами, затримками та можливими цілеспрямованими атаками зловмисників. Це ускладнює процес своєчасного виявлення аномалій та прийняття рішень щодо стану каналу в режимі реального часу.

У зв’язку з цим виникає потреба у створенні інформаційних технологій підтримки рішень, які поєднують методи математичного моделювання, інтелектуального аналізу даних та машинного навчання для забезпечення комплексного моніторингу параметрів квантового каналу. Такі технології повинні не лише виявляти аномальні стани й потенційні загрози, але й формувати аналітичні висновки, що підвищують обґрунтованість та швидкість прийняття рішень у системах квантового розподілу криптографічних ключів.

Актуальність дослідження також визначається необхідністю інтеграції квантових комунікацій у сучасні інформаційні системи та інфраструктури

кібербезпеці. Це потребує нових підходів до побудови архітектур підтримки рішень, здатних адаптуватися до змінних умов функціонування каналу, забезпечувати стійкість до різних типів атак і враховувати специфіку обробки великих обсягів потокових даних.

Значний внесок у систематизацію та класифікацію квантових технологій інформаційної безпеки зробили О. Корченко, Ю. Василюк та С. Гнатюк, які у своїх роботах представили огляд сучасних методів квантового розподілу ключів і показали можливості їх практичного впровадження у реальні телекомунікаційні системи. Дослідження цієї групи стало основою для формування наукової школи, орієнтованої на інтеграцію квантових методів у національну інфраструктуру кіберзахисту.

Подальший розвиток цього напряму відображено у працях І. Бондаренка та Д. Пінчука, які розглядають перспективи квантових телекомунікаційних технологій в Україні та у світі, зокрема в контексті підвищення захищеності критичних інформаційних систем. Автори підкреслюють необхідність адаптації вітчизняної інформаційної інфраструктури до впровадження технологій квантового розподілу ключів.

Особливу увагу у вітчизняній науці приділено також проблемі постквантової криптографії. В. Шекета досліджує питання стійкості існуючих криптографічних протоколів у контексті появи квантових обчислювальних засобів і наголошує на необхідності пошуку нових підходів до побудови криптостійких алгоритмів. Цей напрям тісно пов’язаний із задачею створення систем підтримки прийняття рішень для моніторингу та адаптації безпекових механізмів у квантових каналах.

Важливим фундаментальним підґрунтям для розвитку квантових комунікацій стали дослідження А. Омельянчука, присвячені теорії та експериментальній реалізації джозефсонівських кубітів. Хоча ці роботи спрямовані переважно на фізику надпровідних структур, вони мають безпосередній зв’язок із практичними аспектами розвитку квантових систем, що використовуються у каналах захищеного передавання даних.

Окремо слід відзначити В.О. Устименко який є одним із провідних українських дослідників у галузі постквантової криптології, який запропонував принципово новий підхід до побудови криптосистем, відмінний від класичних алгоритмів з відкритим ключем. Його наукова діяльність зосереджена на розробці криптографічних платформ на основі некумутативних алгебраїчних структур, груп та напівгруп афінних перетворень, а також багатовимірних поліноміальних відображень.

С.В. Зайцев зосереджує наукові дослідження на побудові систем зі структурною та параметричною адаптацією, розробці адаптивного завадостійкого кодування на основі турбокодів, LDPC- та polar-codes, вивченні систем передачі інформації з використанням OFDM, MIMO та розширення спектру сигналів, а також на методах підвищення стійкості криптографічних систем і технічному захисті інформації.

Таким чином, розробка інформаційної технології підтримки рішень у захищених системах квантової передачі інформації є актуальною науково-технічною задачею, що має вагоме значення для розвитку теорії та практики комп'ютерних наук, а також для підвищення рівня інформаційної безпеки державних, наукових і корпоративних комунікаційних мереж.

Об'єкт дослідження. Об'єктом дослідження є процес функціонування системи квантової передачі інформації, що реалізує розподіл криптографічних ключів у каналах оптичного зв'язку. Він включає фізичні, технічні та інформаційні аспекти формування, передачі та обробки квантових станів фотонів у присутності шумів, втрат та потенційних загроз з боку зловмисника.

Предмет дослідження. Предметом дослідження є інформаційна технологія підтримки прийняття рішень у захищеній системі квантової передачі інформації, що охоплює методи, алгоритми та програмні засоби аналізу параметрів квантового каналу зв'язку на основі використання нейронних мереж.

Зокрема, увага зосереджується на розробці та вдосконаленні підходів до:

- формалізації процесів оцінювання стану квантового каналу в умовах наявності шумів, втрат та атак;

- використання методів інтелектуального аналізу даних і машинного навчання для виявлення аномалій у потоці квантових бітів;

- побудови моделей підтримки рішень, здатних адаптивно реагувати на зміни характеристик середовища та забезпечувати стабільний рівень захищеності;

- інтеграції кластерного аналізу, нейромережної моделі і статистичних методів для багаторівневої інтерпретації експериментальних даних.

Наукова новизна одержаних результатів. У дисертаційній роботі отримано результати, що характеризуються науковою новизною та розвивають сучасні підходи до побудови захищених систем передачі інформації з використанням методів інтелектуального аналізу даних та технологій підтримки прийняття рішень, а саме:

1. Вперше розроблена інформаційна технологія підтримки прийняття рішень у сфері надійності передачі інформації, що базується, на відміну від існуючих методів інтерпретації станів потокових даних параметрів каналу, методами кластерного аналізу та класифікації яка реалізується з використанням багатошарової нейронної мережі. Це дозволяє забезпечити можливість автоматичного виявлення аномалій в процесі роботи каналу зв'язку та гарантує доведення надійності передачі інформацій до прийнятного рівня.

2. Удосконалено метод оцінювання стану каналу зв'язку, що включає використання багатокритеріального аналізу фізичних параметрів квантових елементів з урахуванням їхніх кореляційних залежностей. Це дозволяє виявляти ймовірні потенційні аномалії.

3. Удосконалено методи інтеграції машинного навчання з квантовими криптографічними протоколами, що дозволяє реєструвати параметри, виконувати інтелектуальний аналіз у режимі реального часу, виконати процедури машинного навчання, здатних до адаптації в умовах динамічних загроз.

4. Дістав подальший розвиток метод формалізації процедур підтримки прийняття рішень при управлінні каналами передачі інформації із застосуванням принципів потокової обробки багатовимірних статистичних даних, отриманих під час

роботи каналу. Це забезпечує адаптацію налаштування протоколів розподілу ключів відповідно до поточного стану каналу.

Мета і задачі дослідження. Метою дисертаційної роботи є розробка та наукове обґрунтування інформаційної технології підтримки прийняття рішень для управління каналом передачі інформації, в умовах проявлення загроз аномалій та відмов для підвищення стійкості системи до прийнятного рівня.

Для досягнення поставленої мети необхідно вирішити такі наукові та прикладні завдання:

1. Виконати аналітичний огляд сучасних методів забезпечення безпеки у квантових системах передачі інформації при розподілу ключів та підходів до підтримки прийняття рішень у сфері захищених телекомунікацій.

2. Розробити інформаційні моделі та методи статистичного аналізу та кластеризації експериментальних даних квантового каналу для виявлення критичних станів і відокремлення стаціонарний режим, від аномальних.

3. Створити математичні моделі та алгоритми виявлення аномалій у системі квантового розподілу ключів із використанням багатошарової нейронної мережі. Розробити методи емуляції процесів квантової передачі інформації та інструментальні засоби перевірки математичних моделей на симуляції роботи віртуального каналу зв’язку.

4. Розробити інформаційну технологію підтримки рішень, яка інтегрує засоби збору, обробки та інтелектуального аналізу даних у реальному часі для підвищення надійності та безпеки квантових каналів.

5. Провести верифікацію та валідацію розроблених інформаційних моделей та методів на основі симуляції роботи віртуального каналу зв’язку та оцінити ефективність за показниками точності класифікації режимів роботи каналу, обчислювальної складності та часу реакції на аномальні події.

У процесі дослідження розробки та впровадження технології підтримки прийняття рішень у системі квантової передачі інформації було використано комплекс

сучасних методів комп’ютерних наук, математичного моделювання та інтелектуального аналізу даних з використанням нейронної мережі.

Методи дослідження. У процесі дослідження розробки та впровадження інформаційної технології підтримки рішень у системи квантової передачі інформації було використано комплекс сучасних методів комп’ютерних наук, математичного моделювання та інтелектуального аналізу даних.

1. Методи математичного моделювання та симуляції. Для опису процесів у квантовому каналі зв’язку застосовано методи імітаційного моделювання. Це дало змогу відтворити процес генерації та передавання квантових станів у протоколі BB84, змоделювати вплив внутрішніх та зовнішніх завад на параметри сигналу, а також дослідити динаміку зміни Quantum Bit Error Rate (QBER) залежно від фізичних характеристик каналу.

2. Методи статистичного аналізу. Для обробки експериментальних та симуляційних даних використано інструменти описової статистики: розрахунок середнього значення, медіани, дисперсії, стандартного відхилення, коефіцієнта варіації, а також побудову нормалізованих гістограм розподілу. Оцінка кореляційних зв’язків між параметрами (потужність випромінювання, рівень шуму, час прибуття фотонів, коефіцієнт помилок) що дало змогу виявити приховані залежності між характеристиками каналу.

3. Методи кластерного аналізу. Для виявлення закономірностей у багатовимірному просторі ознак використано алгоритми k-means. Це дозволило визначити області нормального функціонування каналу та відокремити аномальні стани, які свідчать про деградацію або потенційні атаки. Кластеризація застосовувалася як на рівні серій переданих квантових бітів, так і на рівні віконних послідовностей для підвищення точності виявлення аномалій.

4. Методи машинного навчання та нейронних мереж. Для задач класифікації станів каналу розроблено багатошаровий перцептрон для аналізу часових послідовностей параметрів. Навчання здійснювалось на основі сформованих вибірок

із симульованих і експериментальних даних. Використано оцінку якості за метриками macro-F1, точності та повноти.

Зв'язок роботи з науковими програмами, планами, темами. Наукові результати дисертації отримані в межах програми науково-дослідних робіт на базі Інституту телекомунікацій і глобального інформаційного простору Національної академії наук України та реалізовані у тематиках: «Розробка засобів інформаційно-аналітичної підтримки завдань забезпечення стійкості об’єктів критичної інфраструктури в регіональній соціоекосистемі за умов зростання природних, техногенних і соціальних загроз» (№ ДР 0121U109216), «Розробка обчислювальних технологій та методів моделювання для дослідження нестаціонарних процесів» (№ РК 0116U000793 державної реєстрації), Закон України «Про національну безпеку України», Стратегія національної безпеки України «Безпека людини – безпека країни» та Концепція розвитку цифрової економіки та суспільства України.

Практичне значення отриманих результатів. Практичне значення отриманих результатів полягає у створенні інформаційної технології підтримки прийняття рішень у системах квантової передачі інформації, яка забезпечує комплексний моніторинг параметрів каналу, своєчасне виявлення аномалій та підвищення достовірності даних. Розроблені математичні моделі, алгоритми та програмні засоби можуть бути використані для оцінювання та управління станом оптичних ліній передачі даних, формування критеріїв безпеки та реалізації адаптивних заходів захисту.

Отримані результати доцільно застосовувати:

- у побудові національних та корпоративних сегментів квантових комунікаційних мереж;

- при проектуванні та випробуванні телекомунікаційних систем критичної інфраструктури, де потрібен високий рівень захищеності даних;

- у сфері банківських та фінансових установ, які впроваджують технології квантового захисту для транзакцій та міжбанківських комунікацій;

- у державних інформаційних системах, що потребують гарантованої конфіденційності (захист дипломатичного та оборонного зв’язку);

- для тестування обладнання та розробки технічних стандартів у галузі квантових мереж.

Особистий внесок здобувача. Усі наукові результати, що виносяться на захист, отримані здобувачем самостійно.

Проведено огляд еволюції протоколів квантового розподілу ключів та класифікацію загроз із аналізом основних атак.

Розроблено математичну модель оцінки відмов і створено імітаційну модель роботи каналу.

Розроблено архітектуру інформаційної технології контролю та класифікації станів з програмною реалізацією.

Розроблено та навчено багатошаровий нейрону мережу для класифікації режимів «stationary/anomaly», проведено експерименти й оцінено ефективність моделі (accuracy, F1, ROC).

У співавторстві уточнено методологічні положення інтеграції статистичних і інтелектуальних методів, підготовлено публікації та акти впровадження результатів.

Апробація результатів дисертації. Основні результати, що отримані у дисертаційному дослідженні доповідались на конференціях:

1. Зінченко, В. Л., & Лифар, В. О. (2024, жовтня). Використання нейронних мереж для оптимізації квантових каналів зв’язку у квантовій криптографії. У Матеріали науково-практичної конференції з інформаційних технологій (м. Миколаїв, Україна). Інформаційні технології: моделі, алгоритми, системи (ITMAS – 2024). С 102-103.

2. Зінченко, В. Л., & Захожай, О. І. (2025, 26 березня). Інформаційна модель виявлення та класифікації атак у квантових каналах зв’язку на основі кластерного аналізу [Тези доповіді]. Innovative Approaches in Modern Science and Technology (Lisbon, Portugal). С. 116–117.

Публікації. За результатами досліджень опубліковано три наукові роботи, що висвітлюють основний зміст дисертації, серед них одна стаття опублікована у міжнародному періодичному виданні, що проіндексовано у базі даних Scopus [53]; дві статті опубліковано у наукових виданнях України (кат. А та кат. Б), що включено до Переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора наук, кандидата наук та ступеня доктора філософії [54, 65].

Дисертаційна робота складається з анотації, вступу, чотирьох розділів, висновків, списку використаних джерел, додатків. Загальний обсяг роботи складає 163 сторінки, серед яких 173 сторінка основного тексту. Робота містить 23 рисунки, 4 таблиці, список використаних джерел із 115 найменувань та 3 додатка.

РОЗДІЛ 1. ОГЛЯД ПРОБЛЕМИ ТА СТАНУ ДОСЛІДЖЕНЬ У СФЕРІ ЗАХИЩЕНОЇ КВАНТОВОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ

1.1 Віхи розвитку квантової криптографії та внесок наукової спільноти

Розвиток квантового розподілу ключів (QKD) за останні десятиліття відбувався поетапно: від перших лабораторних експериментів до створення реальних мережевих прототипів. Основними засадами стали протоколи BB84 та B92, які вперше продемонстрували принципову можливість використання квантових станів для побудови криптографічних ключів. Проте їх практична реалізація виявила низку проблем при передачі, серед яких - обмежена дистанція, вплив шумів та вразливість до атак на джерела та детектори [1]. Ці обмеження стимулювали подальший пошук рішень і сприяли формуванню цілого напряму досліджень з удосконалення протоколів та інженерних рішень.

Одним із ключових методологічних досягнень у розвитку квантової криптографії є застосування decoy-state підходу, що забезпечує ефективний захист від атак типу photon-number-splitting (PNS). Суть методу полягає у введенні додаткових («приманних») варіацій амплітуди випромінювання, що унеможливлює для зловмисника достовірне розрізнення однофотонних та багатофотонних імпульсів. Такий підхід дозволяє здійснити більш коректну оцінку внеску однофотонних сигналів у процес генерації ключа, що, у свою чергу, істотно підвищує стійкість та надійність квантових систем розподілу криптографічних ключів.

Це відкривало шлях до використання QKD на значно більших відстанях і наближало технологію до практичного застосування в телекомунікаційних мережах [2-9]. Таким чином, удосконалення базових протоколів стало основою для подальшого розвитку.

Суттєвим кроком уперед була розробка measurement-device-independent QKD (MDI-QKD). Ця архітектура усуває одну з головних вразливостей системи - можливість атак на детектори, які вважаються «слабким місцем» більшості реалізацій. В MDI-QKD вимірювальний вузол розташовується у недовіреному середовищі, що дозволяє значно знизити ризик компрометації результатів через апаратні атаки. Експериментальні демонстрації підтвердили працездатність підходу навіть за умов нестабільних і асиметричних каналів [10], що зробило MDI-QKD важливим етапом для розвитку безпечних квантових мереж.

Іншим напрямом розвитку стала continuous-variable QKD (CV-QKD), яка отримала особливу увагу завдяки сумісності з існуючою волоконно-оптичною інфраструктурою. На відміну від дискретних протоколів, CV-QKD використовує когерентні стани та гомодинні або гетеродинні вимірювання, що забезпечує можливість застосування стандартних телекомунікаційних компонентів. Експериментальні дослідження з доведенням composable security [11] засвідчили, що CV-QKD може працювати на реалістичних обсягах даних і задовольняти вимоги операторських мереж, наближаючи технологію до практичного впровадження.

Щоб подолати фундаментальні обмеження пропускної здатності, було запропоновано протоколи TF-QKD та PM-QKD. Ці протоколи забезпечують масштабування секретної швидкості за законом $\sim\sqrt{\eta}$ та дозволяють працювати на сотнях кілометрів без квантових ретрансляторів. Їх практичні реалізації показали перспективи використання у магістральних волоконних лініях, проте питання стабілізації фази й боротьби з новими типами атак залишаються відкритими [12].

Не менш важливим напрямом став розвиток вільнопросторових QKD-систем. Якщо перші експерименти обмежувалися нічними умовами, то сучасні дослідження продемонстрували можливість роботи вдень за рахунок поєднання спектральної, часової та просторової фільтрації. Це створило передумови для супутникового QKD, який розглядається як ключовий елемент глобальних безпечних комунікаційних мереж [13, 14].

Поступово QKD перейшов від мереж p2p (point-to-point), експериментів до створення мережевих прототипів. Важливу роль відіграв проект SECOQC у Відні, який продемонстрував можливість побудови міської квантової мережі на основі підходу trusted-repeater [15]. Сучасні ж дослідження орієнтуються на архітектури без довіри до вузлів: зокрема, сегментовані зіркові мережі з одночасними сеансами QKD [17] та MDI-мережі з використанням оптичних гребінок [16]. Це формує основу для сервісної моделі key-as-a-service, яка може інтегруватися з традиційними телекомунікаційними мережами.

Важливо підкреслити, що до розвитку цього напряму активно долучаються й українські науковці. У працях Корченка, Василюка та Гнатюка систематизовано квантові технології інформаційної безпеки та проаналізовано перспективи їх практичного впровадження у національну інфраструктуру [5]. Бондаренко й Пінчук досліджують можливості розвитку квантових телекомунікацій в Україні та визначають виклики інтеграції цих технологій у вітчизняні мережі [17]. Крім того, у працях українських фізиків значна увага приділяється питанням побудови кубітів на основі надпровідних структур, що є важливим підґрунтям для розвитку апаратної бази квантових комунікацій [8]. Таким чином, українська наукова школа робить вагомий внесок у формування міжнародного дискурсу з питань безпеки квантових комунікацій.

Узагальнюючи, можна виділити кілька стратегічних результатів: підвищення практичної безпеки завдяки MDI-QKD, сумісність з телеком-інфраструктурою завдяки CV-QKD, подолання фундаментальних обмежень за допомогою TF/PM-QKD та перехід до масштабованих мережевих архітектур. Водночас залишається низка відкритих питань: фазова стабілізація на великих дистанціях, сертифікація обладнання, узгодження метрик «безпека–продуктивність» та економічна доцільність впровадження. Ці виклики підкреслюють актуальність створення інформаційних технологій підтримки рішень, здатних забезпечити комплексний моніторинг та управління у квантових системах передачі інформації.

1.2. Протоколи та реалізації

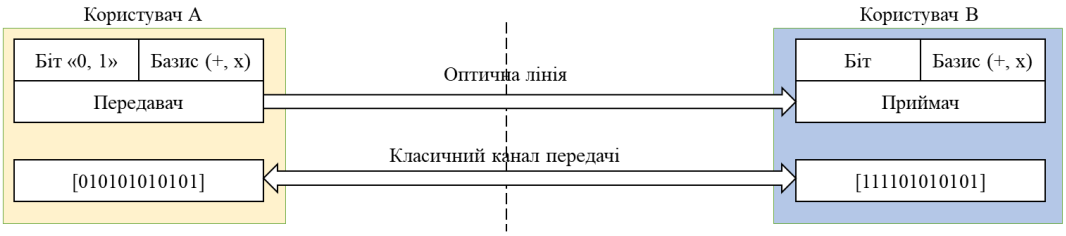
Розвиток протоколів квантового розподілу ключів є фундаментальною основою для побудови захищених систем квантових комунікацій. Кожен з них виникав як відповідь на конкретні практичні проблеми - від обмежень дальності та атак на багатофотонні імпульси до недоліків детекторів та потреби глобального масштабування. Огляд протоколів дозволяє систематизувати їх еволюцію, продемонструвати логіку переходу від одних рішень до інших та виокремити залишкові ризики, що залишаються відкритими. Такий аналіз не лише окреслює сучасний стан досліджень, але й створює підґрунтя для формування інформаційних технологій підтримки рішень, здатних враховувати сильні та слабкі сторони кожного підходу.

1.2.1. Базові протоколи: BB84 та B92

Першими кроками у розвитку квантової криптографії стали протоколи BB84 та B92, які заклали фундамент сучасних систем розподілу ключів. Протокол BB84, запропонований Ч. Беннеттом і Ж. Брассаром у 1984 році, ґрунтувався на використанні чотирьох поляризаційних станів фотонів для передачі випадкових бітів [18].

Основою протоколу BB84 є випадкова генерація бітів та базисів, на основі яких створюються й передаються квантові стани. На стороні користувача A формується послідовність випадкових бітів, кожен з цих бітів кодується у вибраному базисі: прямому (+) або у діагональному (×). Згідно з цим базисом біт переводиться у відповідний стан фотона з певною поляризацією (горизонтальною, вертикальною,

діагональною або антидіагональною). Підготовлені фотони передаються через оптичний канал, рисунок 1.1.



Відправлена серія бітів:	0	1	0	1	0	1	0	1	0	1	0	1	Користувач А
Обраний базис:	+	x	+	+	+	x	x	x	+	x	+	x	
Обраний базис:	x	+	x	+	x	x	x	x	x	+	+	+	Користувач В
Визначені біти	0	1	1	1	0	1	0	1	1	1	0	1	
Узгодження													
Сирий ключ:				1		1	0	1			1		

Рисунок 1.1 - Принцип роботи протоколу BB84

Користувач В для кожного отриманого фотона незалежно обирає базис вимірювання. Якщо вибір базису збігається з базисом, у якому був закодований фотон, то результат вимірювання відтворює початкове значення біта. У випадку розбіжності базисів значення визначається випадковим чином і не використовується у подальшій обробці.

Після завершення передавання сторони через класичний канал обмінюються інформацією про використані базиси, не розкриваючи самих бітів. Ті позиції, де базиси не збіглися, відкидаються. В результаті формується скорочена послідовність, що отримала назву сирий ключ. На схемі червоним кольором позначені відкинуті біти, а зеленим - ті, що збережені після узгодження. Саме ця підпослідовність стає основою для подальших процедур перевірки та посилення секретності.

Протокол B92, запропонований Беннеттом у 1992 році, спростив схему, залишивши лише два неперпендикулярні квантові стани, що зробило реалізацію менш ресурсоємною.

Завдяки цим протоколам вперше було показано, що квантова механіка може забезпечити безумовну секретність ключів, на відміну від класичних криптосистем, стійкість яких залежить від складності математичних задач. Проте практичне впровадження BB84 і B92 виявило низку обмежень. По-перше, реальні джерела світла не є ідеальними однофотонними випромінювачами, що робить систему вразливою до атак, зокрема photon-number-splitting. По-друге, дальність передачі була обмежена втратами у волокні та шумами детекторів. Нарешті, базові side-channel атаки (часові зсуви, засліплення детекторів) могли знизити безпеку системи [19].

Таким чином, базові протоколи виконали свою ключову роль: вони довели принципову реалізовність QKD і дали старт подальшим модифікаціям. Водночас вони підкреслили фундаментальну проблему: реальні системи відрізняються від ідеалізованих моделей, тому безпека має враховувати особливості практичної реалізації.

1.2.2. Протоколи на приманних станах

Подальший розвиток QKD був зумовлений необхідністю вирішення проблеми PNS-атак, що виникають через використання слабкокогерентних джерел світла. У класичному BB84 передавач іноді випромінює багатофотонні імпульси, які зловмисник може використати для розділення фотонів і збереження копії інформації без виявлення. Цей вектор атаки серйозно обмежував безпеку систем на практичних відстанях.

Проривною ідеєю стала пропозиція використати імпульси з різною інтенсивністю - так звані decoy states. Вперше цей підхід описав В. Хван у 2003 році [1], а згодом він був формалізований і розвинений Ло, Ма та Ченом [20]. Суть методу полягає у випадковому чергуванні «сигнальних» та «приманних» станів, що дозволяє статистично оцінити ймовірність багатофотонних подій та виявити втручання

зловмисника. Якщо частка помилок або відхилення інтенсивностей перевищують очікувані значення, це сигналізує про атаку.

Використання decoy-state зробило можливим розширення дистанції QKD до сотень кілометрів у волоконних каналах і значно підвищило швидкість генерації ключа. Більше того, ця технологія стала стандартом у сучасних експериментах і комерційних системах, оскільки не потребує ідеальних джерел однофотонних імпульсів [9].

Втім, метод має й залишкові ризики. Практична реалізація вимагає високої точності калібрування та стабільності джерел, оскільки навіть невеликі флуктуації інтенсивності можуть створювати «вікна можливостей» для атак. Крім того, decoy-state не вирішує проблему side-channel атак, пов’язаних із технічними особливостями детекторів і модуляторів. Саме ці фактори стали мотивацією для подальшого розвитку протоколів, таких як MDI-QKD.

1.2.3. Протокол SARG04

Протокол BB84 у комбінації з приманними станами значно підвищив безпеку дискретних систем, він залишався вразливим до частини атак, пов’язаних із багатофотонними імпульсами. Ця проблема стимулювала пошук альтернативних схем, здатних зберігати секретність навіть у випадку недосконалих джерел. У 2004 році група дослідників під керівництвом Валеріо Скарані запропонувала протокол SARG04 [21]. Його ключова відмінність від BB84 полягає у зміні правила бітової інтерпретації станів: замість прямих відповідностей «стан-біт» використовується оголошення пари можливих станів, серед яких лише один співпадає з реально переданим.

Завдяки цій зміні SARG04 став більш стійким до PNS-атак. Якщо у BB84 зловмисник, отримавши багатофотонний імпульс, може зберегти копію фотона і з

часом дізнатися його стан, то у SARG04 через специфіку бітових правил така стратегія стає менш ефективною. Експериментальні дослідження підтвердили, що протокол демонструє вищу секретну швидкість у сценаріях з високими втратами, де BB84 втрачає стійкість [1].

Водночас SARG04 має обмеження. Його реалізація вимагає складнішої логіки обробки та аналізу помилок, що знижує швидкість генерації ключа в ідеальних умовах. Крім того, у випадку застосування decoy-state-методики, яка вже стала стандартом для BB84, переваги SARG04 зменшуються. Тому в сучасних системах він розглядається радше як варіант для специфічних сценаріїв, ніж як універсальне рішення. Проте внесок SARG04 важливий: він розширив палітру інструментів DV-QKD та показав, що зміна правил інтерпретації станів може підвищити безпеку навіть без радикальної перебудови фізичної частини системи.

1.2.4. Протокол MDI-QKD

Одним із найсерйозніших викликів для практичного QKD стали атаки на детектори. Починаючи з 2010-х років, експериментально продемонстровано низку методів компрометації, серед яких detector blinding, time-shift атаки та інші side-channel впливи [22], що підтверджує вразливість практичних реалізацій квантових протоколів.

Революційне рішення запропонували Х.-К. Ло, М. Керті та Б. У 2012 році, представивши архітектуру measurement-device-independent QKD (MDI-QKD) [23]. Її суть полягає в тому, що обидва користувачі (Аліса і Боб) надсилають свої стани у спільний недовірений вузол, де виконується Bell-state measurement (BSM). Навіть якщо цей вузол контролює зловмисник, він не отримує доступу до секретного ключа, оскільки інформація формується лише на основі кореляцій результатів вимірювання, а не конкретних детекторних подій.

Експериментальні реалізації швидко підтвердили працездатність MDI-QKD. Зокрема, у 2018 році було продемонстровано стабільну роботу протоколу у каналах з асиметричними втратами та нестабільними параметрами [10]. Подальші дослідження показали можливість генерації ключів на сотнях кілометрів із використанням сучасних оптичних компонентів [24]. Ці результати довели, що MDI-QKD є ефективною відповіддю на клас атак на детектори, який вважався однією з найсерйозніших практичних загроз для QKD.

Проте і цей підхід має залишкові ризики. По-перше, він значно складніший у технічній реалізації: потрібна високоточна синхронізація двох незалежних джерел світла, стабілізація фазових та часових параметрів каналів. По-друге, MDI-QKD не усуває всіх можливих side-channel атак на джерела (наприклад, витоки через інтенсивність або фазу лазера). Тому дослідження останніх років зосереджені на поєднанні MDI-QKD із іншими методами захисту, зокрема з decoy-state технікою та сертифікацією джерел [25].

Загалом MDI-QKD стало ключовою віхою у розвитку QKD. Воно дозволило перетворити найбільш вразливу частину системи — детектори — на «чорну скриньку», до якої не потрібно мати довіру. Ця концепція суттєво підвищила рівень практичної безпеки і заклала основу для подальших розробок багатокористувацьких квантових мереж, де центральний вузол може бути недовіреним.

1.2.5. Протокол CV-QKD

З розвитком дискретних протоколів у спільноті сформувався напрям CV-QKD (continuous-variable QKD), що вирішує проблему інтеграції квантових каналів у вже наявну волоконно-оптичну інфраструктуру. Його ключова ідея полягає у використанні когерентних станів світла та вимірювань квадратичних компонент електромагнітного поля за допомогою гомодинних чи гетеродинних детекторів [26]. Завдяки цьому CV-

QKD може використовувати стандартні телекомунікаційні компоненти (лазери, модулятори, приймачі), що значно знижує бар’єри впровадження технології.

Практична перевага CV-QKD полягає у вищих швидкостях генерації ключів на малих і середніх відстанях. Оскільки метод використовує багатофотонні когерентні стани, вдається отримати значний обсяг даних для статистичного аналізу, що підвищує ефективність протоколу. Однак це ж робить CV-QKD чутливим до шумів каналу та втрат, які зростають із відстанню. Тому довгий час протокол вважався перспективним, але недостатньо зрілим для реального використання у магістральних мережах.

Ключовим проривом стало доведення composable security для CV-QKD на реалістичних обсягах даних. У 2022 році було продемонстровано роботу системи з обробкою близько 2×10^8 когерентних станів і доведенням стійкості проти колективних атак [27]. Це дозволило вважати CV-QKD не лише теоретично цікавим, а й практично придатним для мереж операторського рівня. Сучасні експерименти також показують, що CV-QKD здатний забезпечити швидкість генерації секретного ключа на рівні сотень мегабітів за секунду у міських мережах [12].

Незважаючи на ці досягнення, CV-QKD має залишкові ризики та обмеження. По-перше, протокол вимагає ретельної калібровки локальних осциляторів і стабільності фаз, що підвищує вимоги до апаратного забезпечення. По-друге, безпека CV-QKD значною мірою базується на асимптотичних оцінках і вимагає великих вибірок для статистично значущих результатів. Це обмежує швидкість реагування на аномалії в реальному часі. Нарешті, на відміну від MDI-QKD, CV-QKD не усуває вразливості детекторів, тому питання side-channel атак залишаються актуальними.

Загалом CV-QKD став важливою ланкою у розвитку квантових комунікацій. Він демонструє можливість поєднання високої швидкості з використанням існуючої інфраструктури, що робить його привабливим для комерційних застосувань. Водночас залишкові проблеми підкреслюють потребу у системах підтримки рішень, здатних оперативно виявляти та аналізувати вплив шумів, дрейфів і потенційних атак у реальному часі.

1.2.6. Протокол TF/PM-QKD

Іншим великим кроком у розвитку QKD стала поява протоколів, здатних подолати фундаментальну межу пропускання каналів, відому як PLOB bound [28]. Згідно з цим обмеженням, секретна швидкість у традиційних протоколах знижується пропорційно коефіцієнту пропускання каналу η. Це означало, що без використання квантових повторювачів збільшити відстань QKD було практично неможливо.

Прорив стався у 2018 році, коли Ма, Цзен і Чжоу запропонували протокол PM-QKD (Phase-Matching QKD) [31]. Його суть полягає у використанні когерентних станів із випадковими фазами, які потім узгоджуються між сторонами. Завдяки цьому вдається досягти масштабування секретної швидкості $\sim\sqrt{\eta}$ замість η, що істотно перевищує класичні обмеження. Незалежно від цього було розроблено протокол TF-QKD (Twin-Field QKD), який реалізує схожу ідею на базі інтерференції сигналів від двох користувачів у центральному вузлі. Подальші дослідження довели еквівалентність цих підходів і забезпечили формальні докази безпеки [29].

Експериментальні реалізації TF/PM-QKD продемонстрували можливість розширення дистанції QKD до понад 500 км без застосування квантових повторювачів [30]. Це стало важливою віхою для побудови магістральних квантових мереж, які раніше вважалися можливими лише з використанням складних і дорогих повторювальних технологій. Крім того, TF-QKD відкрив перспективи для побудови глобальних ліній на базі існуючої оптичної інфраструктури.

Водночас протоколи TF/PM-QKD мають залишкові проблеми. По-перше, вони вимагають надзвичайно точної фазової стабілізації між віддаленими джерелами світла, що є складним завданням у польових умовах. По-друге, реалізації досі залишаються складними й дорогими, що обмежує їх комерційне застосування. Нарешті, новизна підходів означає, що вони ще недостатньо перевірені на практиці проти всіх можливих векторів атак, включаючи side-channel впливи.

Отже, TF/PM-QKD стали революційним кроком у подоланні фундаментальних обмежень квантових каналів. Вони відкрили можливість реалізації магістральних ліній без повторювачів і створили основу для майбутніх глобальних мереж QKD. Водночас складність реалізації та залишкові ризики підкреслюють потребу у додаткових механізмах моніторингу та підтримки рішень, що є критично важливим для впровадження цих протоколів у реальних умовах.

1.2.7. Вільнопросторовий та супутниковий QKD

Ще одним напрямом розвитку квантової криптографії є використання вільнопросторових та супутникових каналів, покликаних вирішити проблему глобального охоплення, яке неможливо досягти лише з використанням оптоволокна. Втрати у волоконних каналах зростають експоненційно з відстанню, що обмежує практичний діапазон систем навіть у разі використання передових протоколів на рівні кількох сотень кілометрів. Саме тому ідея застосування супутників як ретрансляторів або безпосередніх учасників квантового зв’язку стала стратегічним кроком у розвитку QKD [31].

Перші наземні експерименти з вільнопросторовими каналами довели принципову можливість передавання квантових станів через атмосферу. Проте такі системи були чутливими до погодних умов, турбулентності та фону сонячного світла. Довгий час експерименти проводили лише вночі. Прорив стався у 2018 році, коли група дослідників продемонструвала можливість денного функціонування QKD завдяки комбінації спектральної, часової та просторової фільтрації шумів [32]. Подальші експерименти показали стабільність роботи навіть у складних атмосферних умовах [33].

Найбільш значущим кроком стало створення у Китаї супутника Micius, який у 2017 році здійснив перші успішні експерименти із супутниковим QKD на відстані

понад 1200 км [31]. У цих експериментах реалізовано як дискретні протоколи (BB84), так і ентанглмент-базовані схеми, що підтвердило можливість побудови глобальних мереж. Важливо, що супутникові QKD-лінки вже інтегрувалися з наземними волоконними системами, створюючи гібридні архітектури, здатні забезпечити трансконтинентальне поширення ключів [34].

Попри ці успіхи, вільнопросторові та супутникові системи мають залишкові обмеження. По-перше, вони залежать від погодних умов та потребують складної системи наведення та відстеження оптичних каналів. По-друге, висока вартість запуску та обслуговування супутників обмежує широке впровадження технології. По-третє, забезпечення безпеки у багатокористувацьких сценаріях і сертифікація компонентів (наприклад, бортових модулів супутників) залишається відкритим завданням. Тому на сучасному етапі супутниковий QKD розглядається як доповнення до волоконних мереж, а не як їхня заміна.

Усі розглянуті протоколи квантового розподілу ключів мають різні цілі, обмеження та практичні особливості. Для системного аналізу доцільно представити їх у порівняльній формі, що дозволяє чітко побачити, яку проблему кожен протокол вирішує. Результати порівняння цих протоколів наведе у таблиці 1.

Таблиця 1.1 – Протоколи квантового розподілу ключів, їхні проблеми, рішення та залишкові ризики

Протокол	**Проблема**	**Рішення**	**Залишковий ризик**
BB84/B92	Потреба в доведеній безпеці; слабкості через багатофотонні імпульси	Використання поляризаційних станів (BB84) та двох неперпендикулярних станів (B92)	Обмежена відстань передачі, чутливість до завад, атаки на реалізацію
Decoy-state	Атаки PNS у слабкокоерентних джерелах	Використання імпульсів різної інтенсивності для статистичного контролю	Вимоги до стабільності джерел випромінювання.
SARG04	Обхід PNS-атак у BB84	Інша бітова інтерпретація станів	Нижча швидкість генерації ключів

MDI-QKD	Атаки на детектори (blinding, time-shift)	Bell-state measurement у недовіреному вузлі	Висока технічна складність.
CV-QKD	Інтеграція з телеком-інфраструктурою	Когерентні стани, гомо/гетеродин, DSP	Чутливість до завад; великі вибірки для безпеки; side-channel у детекторах
TF/PM-QKD	Фундаментальне обмеження PLOB	Інтерференція когерентних станів; узгодження фаз	Вимоги до фазової стабілізації; висока складність реалізації
Free-space / Satellite QKD	Неможливість глобального охоплення у волокні	Використання атмосферних каналів і супутників	Атмосферні втрати; залежність від погоди; висока вартість

1.3 Загрози та контрзаходи

Хоча протоколи квантового розподілу ключів мають доведену теоретичну безпеку, їхні практичні реалізації залишаються вразливими до низки атак. Ці загрози зумовлені відмінністю реальних компонентів від ідеалізованих моделей, що підтверджується численними міжнародними дослідженнями та класифікаціями.

1.3.1. Атака на багатофотонні імпульси

Однією з перших практичних загроз для протоколів дискретних змінних стала атака на багатофотонні імпульси, відома як Photon-Number Splitting (PNS). Вона зумовлена тим, що в реальних системах неможливо використовувати ідеальні однофотонні джерела, а слабкі когерентні лазери іноді випромінюють кілька фотонів одночасно. Зловмисник може перехопити один із них і зберегти для подальшого аналізу, пропускаючи решту до приймача. У такому випадку статистика помилок не змінюється, а секретність ключа фактично порушується. Це суттєво обмежувало можливість використання базового протоколу BB84 на великих відстанях [35].

Відповіддю на цю проблему стало запровадження концепції приманних станів (decoy-state), незалежно запропонованої у працях Хвана (2003) та Ло, Ма й Чена (2005). Ідея полягала у випадковому чергуванні імпульсів різної інтенсивності, що унеможливлювало приховане застосування PNS-стратегії. Статистичний аналіз частоти проходження «сигнальних» та «приманних» станів дозволяє виявити втручання зловмисника, і саме ця методика відкрила шлях до збільшення довжини квантових каналів до сотень кілометрів [36, 37].

Разом із тим, як відзначають українські дослідники (Корченко, Василюк та Гнатюк, 2010), навіть поява decoy-state методів не знімає всіх ризиків: на практиці залишається проблема точного калібрування джерел, нестабільності інтенсивності та можливих побічних каналів. У своїй класифікації атак вони підкреслили, що PNS є лише однією з ланок у ширшому спектрі загроз для протоколів, які охоплюють як атаки на джерела та детектори, так і інформаційні витоки у допоміжних каналах [38]. Таким чином, хоча методика приманних станів значною мірою нейтралізувала PNS, вона стала також поштовхом для систематизації атак та пошуку комплексних підходів до захисту.

1.3.2. Атака спрямована на вразливості детекторів

Однією з найсерйозніших практичних вразливостей протоколів QKD стали атаки на детектори. У теоретичних моделях детектори розглядаються як ідеальні пристрої, що коректно реєструють квантові стани. Проте в реальних системах вони працюють у лавинному режимі і можуть бути навмисно виведені з робочої області. У 2010 році було продемонстровано так звану атаку detector blinding, коли потужний лазерний імпульс переводив лавинні фотодетектори у класичний лінійний режим [22]. У такому стані зловмисник отримував можливість контролювати результати

вимірювань, не викликаючи підозрілих рівнів помилок у ключі. Подібні атаки saturation-типу ґрунтуються на перевантаженні детекторів надлишковим оптичним потоком, що також веде до спотворення статистики.

Поява цього класу атак поставила під сумнів безпеку навіть комерційних QKD-систем, оскільки продемонстровано, що їх можна реалізувати відносно простими технічними засобами. У відповідь спільнота розробила низку контрзаходів. До них належать апаратні рішення (наприклад, оптичні запобіжники й монітори потужності на вході), протокольні зміни (випадкові зміщення порогів детекції) та архітектурні підходи, зокрема MDI-QKD, що взагалі виносить вузол вимірювань у недовірене середовище [23].

Водночас повного усунення ризиків не досягнуто. Як підкреслюють українські дослідники, атаки на детектори належать до класу side-channel загроз, які виникають через розбіжність між ідеальною математичною моделлю протоколу та реальними фізичними компонентами [5]. Навіть за наявності технічних бар’єрів можливі нові варіанти експлуатації нелінійностей у режимі роботи лавинних фотодіодів, що вимагає постійного вдосконалення засобів моніторингу та стандартизації процесів сертифікації обладнання.

1.3.3. Атака часовим зсувом

Ще одним важливим класом практичних загроз для систем квантового розподілу ключів стали атаки, що використовують недосконаліть часової та фазової синхронізації в реальних каналах. У теоретичній моделі передбачається, що кожен фотон реєструється з однаковою ймовірністю незалежно від моменту його надходження чи фазових коливань. Проте в реальних приймачах лавинні фотодіоди мають скінченні часові вікна чутливості, а фазові модулятори схильні до невеликих

систематичних зсувів. Ці особливості стали підґрунтям для розробки так званих time-shift та phase-remapping атак.

У 2008 році Фу та співавтори показали, що зловмисник може зміщувати час приходу фотонів таким чином, щоб підвищити ймовірність їх реєстрації в одному з детекторів, знижуючи ефективність іншого [38]. Це дає змогу збільшити власну інформацію про ключ без істотного зростання показника QBER. Подібним чином phase-remapping атака, вперше описана Фан-Юн Ченом та колегами, використовує той факт, що у практичних системах фазові зсуви не є ідеально рівними. Зловмисник може підбирати власні сигнали так, щоб спотворювати інтерпретацію переданих станів і отримувати часткову інформацію без відчутних помилок [39].

У відповідь на ці загрози були запропоновані різні контрзаходи. Серед них - калібрування часових вікон детекторів, випадкове зміщення моменту відкриття вікна, введення додаткових моніторингових каналів, а також ретельна стабілізація фазових модуляторів. У пізніших роботах було показано, що використання MDI-QKD дозволяє суттєво зменшити ризик time-shift атак, адже результати вимірювань формуються в центральному вузлі й не залежать від конкретних характеристик детекторів [23].

Водночас дослідники, включно з українськими науковцями, підкреслюють, що часові та фазові атаки належать до категорії тонких side-channel впливів, які важко повністю усунути навіть при впровадженні сучасних протоколів [5]. Причина полягає в тому, що будь-які дрейфи чи коливання у фазовій стабілізації можуть бути використані як «шумові вікна» для атак, особливо у довгих магістральних лініях. Тому захист від time-shift та phase-remapping атак сьогодні сприймається не як локальна проблема, а як завдання постійного моніторингу й автоматизованої підтримки рішень у реальному часі.

1.3.4. Атака троянський кінь

Окрему категорію практичних загроз у системах QKD становлять так звані троянський кінь атаки. Їхня суть полягає в тому, що зловмисник не намагається безпосередньо перехопити передані фотони, а вводить у систему додаткове випромінювання - зазвичай лазерні імпульси з іншої довжиною хвилі чи інтенсивністю. Відбившись від елементів передавача (наприклад, фазових або поляризаційних модуляторів), це випромінювання може нести інформацію про встановлені параметри, що дає змогу отримати відомості про вибрані базиси або навіть конкретні біти [40].

Атаки троянський кінь були експериментально продемонстровані у різних лабораторних системах QKD і визнані одними з найбільш небезпечних, оскільки вони експлуатують зворотні витоки сигналу з обладнання. Додаткову складність становить те, що такі атаки важко виявити стандартними методами аналізу QBER, адже вони не обов’язково викликають суттєве зростання рівня помилок.

Контрзаходи проти атак троянського коня здебільшого мають апаратний характер. До них належать оптичні ізолятори, які блокують зовнішнє випромінювання на вході системи, вузькосмугові фільтри, що пропускають лише потрібну довжину хвилі, а також монітори вхідної потужності. Крім того, рекомендується вводити протокольні тести - наприклад, випадкові калібрувальні перевірки інтенсивності та спектра вхідних сигналів [41].

Водночас, троянський кінь належить до класу атак на фізичну реалізацію протоколів, які можуть бути нейтралізовані лише комплексним підходом. Ізоляція чи фільтрація не гарантує повної захищеності, оскільки в системі завжди залишаються допоміжні канали витоку (наприклад, відбиття у волокнах або електромагнітні наводки). Тому сучасна практика передбачає поєднання кількох захисних механізмів та постійний моніторинг вхідного оптичного каналу. Саме цей клас атак ще раз підкреслює важливість створення інформаційних технологій підтримки рішень,

здатних аналізувати багатовимірні параметри й виявляти навіть непрямі ознаки несанкціонованого впливу.

1.3.5. Intercept-resend атаки

Однією з найпростіших і водночас концептуально важливих загроз для квантових протоколів є intercept-resend атака. У цьому випадку зловмисник (традиційно - «Єва») перехоплює кожен фотон, проводить власне вимірювання у випадковому базисі, а потім надсилає до приймача новий фотон у відповідному стані. Якщо обраний базис збігається з базисом передавача, інформація про біт відновлюється без помилок; якщо ж ні - вносяться похибки, які призводять до зростання QBER.

Теоретично саме на здатності виявляти такі атаки й ґрунтується безпека базових протоколів BB84 та B92: якщо QBER перевищує порогове значення, сторони припиняють використання каналу. Проте в реальних умовах проблема полягає в тому, що інші фактори - шум, втрати, нестабільність оптичного тракту - також спричиняють зростання QBER. Це ускладнює розрізнення між природними похибками та діями зловмисника, що створює «сіру зону» для потенційних атак.

Дослідження показали, що класичний intercept-resend може бути вдосконалений за рахунок більш витончених стратегій: наприклад, адаптивного вибору базисів, використання попереднього аналізу стану сигналів або комбінації з часовими зсувами. Такі методи дозволяють зменшити додатковий QBER і збільшити інформацію, яку отримує зловмисник [42]. З іншого боку, сучасні контрзаходи включають використання посилених тестових вибірок, суворіших порогових критеріїв, а також розробку протоколів із більшою стійкістю до шумів (MDI-QKD, CV-QKD).

Атаки типу intercept-resend демонструють фундаментальний принцип: безпека QKD не є абсолютною, вона завжди залежить від співвідношення між рівнем завад у

каналі та точністю статистичного контролю. Це означає, що для реальних систем критично важливо впроваджувати інформаційні технології підтримки рішень, які дозволяють аналізувати параметри каналу у динаміці й відокремлювати випадкові відхилення від цілеспрямованих атак.

Для систематизації розглянутих загроз доцільно узагальнити їх у вигляді порівняльної таблиці. Такий формат дозволяє наочно показати механізми атак, їхні прояви у параметрах квантового каналу, типові контрзаходи та залишкові ризики. Це, у свою чергу, створює підґрунтя для визначення вимог до майбутніх інформаційних технологій підтримки рішень, які мають враховувати комплексну природу практичних атак (див. таблиця. 1.2).

Таблиця 1.2 - Основні атаки на протоколи QKD, їхні механізми, симптоми та контрзаходи

Атака	**Механізм впливу**	**Симптоми у параметрах**	**Основні контрзаходи**	**Залишковий ризик**
Photon-Number Splitting (PNS)	Використання багатофотонних імпульсів для збереження копії стану	Непрямо впливає на статистику проходження імпульсів різної інтенсивності	Decoy-state протоколи	Вимоги до точності калібрування джерел; можливі side-channel витоки
Detector blinding / saturation	Переведення лавинних фотодетекторів у класичний режим за допомогою потужного випромінювання	Зниження випадковості подій; відсутність характерного зростання QBER	Оптичні ізолятори, монітори потужності, MDI-QKD	Нові варіанти атак на нелінійності APD; потреба сертифікації
Time-shift / phase-remapping	Використання різної ефективності детекторів у часі; фазові дрейфи у модуляторах	Асиметрія у реєстрації; приховані систематичні зсуви	Випадкове зміщення вікон; фазова стабілізація; MDI-QKD	Залишкові вразливості при дрейфах у магістральних лініях

Trojan-horse	Ін’єкція зовнішнього випромінювання в канал із витоком інформації від відбиттів	Можливі аномальні коливання потужності; спектральні «сліди»	Оптичні ізолятори, фільтри, монітори потужності	Не повністю усуває витоки; потреба комплексного моніторингу
Intercept-resend	Перехоплення фотонів, вимірювання та повторна передача	Зростання QBER; однак важко відрізнити від шумів каналу	Нові протоколи (MDI, CV)	Складність розрізнення «шум–атака»; потреба у СППР

1.4 Методи контролю та аналізу даних у квантових каналах

Ефективність виявлення аномалій у квантових каналах безпосередньо залежить від того, які методи спостереження та аналітики застосовуються для обробки експериментальних даних. Оскільки загрози, описані у попередньому підрозділі, проявляються через зміну статистичних характеристик сигналу — таких як рівень помилок (QBER), співвідношення сигнал/шум (SNR), часові затримки або інтенсивність імпульсів, - критично важливо мати інструменти, що дозволяють своєчасно ідентифікувати відхилення від норми. У сучасних дослідженнях виділяють чотири основні групи методів: порогові критерії та операційні правила, статистичний аналіз, методи кластеризації та алгоритми машинного навчання. Кожна з цих груп має свої сильні та слабкі сторони, і саме їх порівняння дозволяє сформувати вимоги до майбутніх систем підтримки рішень у сфері квантових комунікацій.

1.4.1 Порогові методи та операційні правила

Найпростішим підходом до виявлення атак у QKD є використання порогових методів. Їхня суть полягає у тому, що ключові параметри каналу — передусім Quantum Bit Error Rate (QBER) - порівнюються з наперед визначеним порогом. Якщо виміряне значення перевищує допустимий рівень (зазвичай 11% для BB84 у випадку оптимального виправлення помилок і приватного підсилення), то канал вважається скомпрометованим і сесія ключового обміну анулюється [43]. Цей підхід забезпечив практичну основу для перших реалізацій QKD, оскільки дозволяв чітко розділити «безпечний» та «небезпечний» режими роботи системи.

Проте подальші експерименти показали, що орієнтація лише на середній рівень QBER є недостатньою. По-перше, різні типи атак можуть призводити до мінімальних змін QBER, залишаючись невиявленими. По-друге, природні шуми каналу, нестабільність лазерів і детекторів також можуть підвищувати QBER, що збільшує кількість помилкових спрацьовувань. Тому у практиці були введені додаткові операційні правила, які враховують не лише загальний рівень помилок, а й динаміку їх зміни, кореляції між параметрами, а також часові вікна, у яких відбувається аномалія [44].

У сучасних системах порогові методи доповнюються інструментами оперативного моніторингу. Наприклад, у комерційних реалізаціях передбачено не лише контроль QBER, а й перевірку стабільності потужності імпульсів, відгуку детекторів та співвідношення сигнал/шум. Це дозволяє швидко зупинити роботу системи при відхиленні від номінальних характеристик, мінімізуючи ризик компрометації. Водночас наукові огляди підкреслюють, що порогові критерії залишаються надто грубим інструментом: вони дають чітку «сигналізацію» лише при значних відхиленнях, тоді як більш тонкі атаки залишаються непоміченими. Саме ця обставина стала мотивацією для розвитку статистичних і кластерних методів, які

дозволяють виявляти приховані залежності у даних та підвищувати чутливість системи [1, 43].

1.4.2 Статистичні методи аналізу

Порогові критерії дають змогу виявляти грубі аномалії у квантовому каналі, однак вони практично не відображають тонкі зміни у параметрах сигналу. Для підвищення чутливості та зменшення кількості хибних спрацьовувань у QKD-системах почали застосовувати методи статистичного аналізу. Вони базуються на обчисленні та відстеженні характеристик вибірок: середнього значення, дисперсії, стандартного відхилення, коефіцієнта варіації, а також на побудові довірчих інтервалів для оцінки стабільності ключових показників каналу [44].

Застосування статистики дає змогу аналізувати не лише інтегральні показники, а й динаміку розподілів параметрів. Наприклад, для QBER важливо не лише його середнє значення, але й поведінка гістограми та асиметрія розподілу. Виявлення зміни форми розподілу може сигналізувати про появу прихованої атаки, навіть якщо середній рівень помилок залишається в межах порогу. Подібним чином аналіз кореляцій між параметрами (потужністю імпульсів, часом прибуття фотонів, рівнем шуму) дозволяє виявляти залежності, які нехарактерні для нормальної роботи каналу [1].

У низці сучасних робіт було показано, що статистичні методи забезпечують ефективний моніторинг навіть у реальних магістральних мережах. Наприклад, під час випробувань у 200-кілометрових волоконних каналах використання розширеного набору статистичних показників дозволило своєчасно фіксувати деградацію сигналу та відокремлювати природні втрати від потенційних аномалій [24].

Таким чином, статистичний аналіз є важливим кроком уперед порівняно з простими пороговими критеріями, проте він не вирішує всіх проблем. Ці обмеження

стимулювали перехід до методів кластеризації, які поєднують статистичні підходи з некерованим машинним навчанням і дозволяють працювати з багатовимірними просторами ознак.

1.4.3. Кластеризація та некероване навчання

Попри ефективність статистичних методів, вони здебільшого працюють з окремими параметрами каналу і не завжди дозволяють врахувати багатовимірну природу даних у QKD. На практиці ж маємо одночасні вимірювання кількох характеристик - потужності імпульсів, часу прибуття фотонів, співвідношення сигнал/шум, рівня помилок, фазових зсувів. У такій ситуації природним підходом є застосування кластеризації та методів некерованого навчання, що дозволяють виявляти приховані закономірності у багатовимірних вибірках без попереднього знання класів [45, 46].

Найчастіше у дослідженнях використовують алгоритм k-means, який ділить простір ознак на кластери за критерієм мінімізації відстані до центроїдів. Додатково застосовуються індекси якості кластеризації, зокрема силуетний коефіцієнт, які допомагають кількісно оцінити ступінь відокремленості груп.

Разом із тим кластеризація має і обмеження. По-перше, методи на кшталт k-means передбачають фіксовану кількість кластерів, що не завжди відповідає реальним умовам. По-друге, результати можуть бути чутливими до початкових умов і масштабу ознак. По-третє, некеровані алгоритми не завжди дають однозначну інтерпретацію: потрібно додатково пояснювати, який із кластерів відповідає нормі, а який - аномалії.

1.4.4 Методи машинного навчання та нейронні мережі

Подальший розвиток підходів до аналізу даних у квантових каналах зумовив активне застосування методів машинного навчання (ML) та нейронних мереж (NN). Якщо кластеризація дозволяє виявляти групи даних без попередньої інформації про їхню природу, то алгоритми з учителем здатні навчатися на попередньо розмічених вибірках і більш точно класифікувати нові стани системи. Це відкриває перспективи для створення моделей, що в режимі реального часу здатні розрізняти нормальну роботу каналу, випадкові збої та потенційні атаки.

Найбільш поширеним напрямом є використання багатошарових нейрона мережа (MLP), які добре працюють із багатовимірними статистичними ознаками. У низці робіт показано, що MLP та інші архітектури нейронних мереж, навчені на характеристиках квантового каналу (середніх значеннях, дисперсіях, коефіцієнтах кореляції), можуть досягати високої точності класифікації станів.

Разом з тим, методи ML/NN мають і обмеження. Їхня ефективність залежить від обсягу та якості навчальних вибірок, які у квантових системах зібрати складно й дорого. Крім того, вони можуть бути чутливими до перенавчання та вимагати значних обчислювальних ресурсів. Важливим викликом залишається і проблема пояснення результатів: складні моделі часто працюють як «чорні скриньки», що ускладнює сертифікацію їхнього використання у критично важливих інфраструктурах [47, 48].

Таким чином, застосування машинного навчання та нейронних мереж у QKD є перспективним напрямом, який підвищує точність і швидкодію систем моніторингу. Проте для їхнього впровадження у практичні протоколи необхідні додаткові дослідження, спрямовані на створення репрезентативних датасетів, розробку моделей, а також інтеграцію із класичними статистичними та кластерними методами.

1.5 Інформаційні технології контролю в існуючих QKD-системах

Практичні реалізації квантового розподілу ключів у світі демонструють різні підходи до забезпечення достовірності інформації, але здебільшого їх об’єднує залежність від порогових статистичних критеріїв. Наприклад, у системі ID Quantique Clavis XG контроль стану каналу базується на безперервному вимірюванні квантової бітової похибки та втрат сигналу перевищення порогового рівня автоматично інтерпретується як загроза безпеці, а система переходить у захисний режим [49]. Аналогічно, рішення Toshiba QKD System застосовують фазову модуляцію та decoy-стани, але принцип ухвалення рішень зводиться до калібрування фотонних трактів і порівняння поточних параметрів з еталонними [50]. Китайська національна мережа QKD (Quantum CTek), яка охоплює понад 2000 км від Пекіна до Шанхаю, використовує модель трастових вузлів: достовірність каналу гарантується тим, що вузол вважається довіреним, а контроль параметрів каналу знову ж таки спирається на статистику помилок [51]. Європейська ініціатива EuroQCI формує гібридну архітектуру, де QKD поєднується з постквантовою криптографією (PQC) для підвищення стійкості, проте у відкритих документах ЄС вказується, що методи моніторингу залишаються класичними й не враховують складних кореляційних зв’язків між параметрами каналу [52].

Висновки до Розділу 1

Еволюція квантового розподілу ключів (QKD) показала поступовий перехід від базових протоколів BB84 та B92 до сучасних архітектур, здатних долати як практичні, так і фундаментальні обмеження. Запровадження методики приманних станів (decoy-state) дало змогу нейтралізувати PNS-атаки й розширити дистанцію передачі, а протокол SARG04 продемонстрував стійкість до багатофотонних імпульсів.

Важливою віхою став розвиток MDI-QKD, що усунув вразливість детекторів, тоді як CV-QKD забезпечив сумісність із телекомунікаційною інфраструктурою та високі швидкості на середніх дистанціях. Проривними стали протоколи TF/PM-QKD, які подолали межу PLOB і відкрили перспективи магістральних ліній без повторювачів, а супутникові системи підтвердили можливість глобального охоплення.

Разом з тим, практичні реалізації залишаються вразливими до широкого спектра атак на джерела та детектори (PNS, blinding, time-shift, Trojan-horse), що доводить: навіть доведена теоретична безпека не гарантує захищеності на практиці. Ці виклики підкреслюють потребу у створенні інформаційних технологій підтримки рішень, які, спираючись на статистичний аналіз, кластеризацію та машинне навчання, здатні забезпечити адаптивний моніторинг квантових каналів, відокремлювати природні флуктуації від цілеспрямованих атак і підвищувати достовірність переданої інформації. [53-54].

РОЗДІЛ 2. МОДЕЛІ І МЕТОДИ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ НА ОСНОВІ АНАЛІЗУ ПРОЦЕСІВ РОБОТИ КАНАЛУ ЗВ'ЯЗКУ

2.1 Загальні положення та концептуальна постановка задач дослідження

Для вирішення поставленої науково-технічної проблеми пропонується розробка та впровадження методу імітаційного динамічного моделювання подій в абстрактному каналі зв'язку. Цей метод дозволить формалізувати та класифікувати причинно-наслідкові зв'язки квантових носіїв у досліджуваних каналах, що є критично важливим для подальшого аналізу та оптимізації систем зв'язку.

Використання сучасних інформаційних технологій у системах підтримки прийняття рішень веде до стрімкого зростання вимог до кібернетичної безпеки. Одним з найбільш перспективних напрямків у цій сфері є криптографічні системи, що базуються на квантовій передачі інформації. Квантова інформатика, як швидко розвиваюча галузь, ґрунтується на абстрактних механізмах отримання, зберігання, передачі та перетворення інформаційних потоків відповідно до законів квантової механіки. Основою математичного апарату квантової інформатики є матричний та оперативний аналіз, а також ймовірнісний аналіз систем нечіткої логіки.

Квантово-механічні ефекти, що проявляються в оптоелектронних системах, мають істотний вплив на фотонний обмін інформацією. Когерентні джерела оптичних квантових генераторів (ОКГ) створюють фотонні потоки з однаковими частотами та фазами, що володіють специфічними фізичними властивостями, такими як заданий спін або квантово заплутаний стан. Це забезпечує можливість адаптивного контролю стану інформаційного середовища, що, в свою чергу, дозволяє здійснювати абсолютний контроль управління інформаційними потоками та захист даних від несанкціонованого доступу.

Для забезпечення надійності та захищеності інформаційних систем пропонується вдосконалення криптографічного захисту у поєднанні з інтелектуальним аналізом стану інформаційного середовища. Це досягається за рахунок використання якісних систем діагностики інформаційних перетворень та гібридних методів, що поєднують квантово-механічні явища з інтелектуальними системами криптографічного захисту.

Квантові комунікаційні канали забезпечують ефективний захист від спроб несанкціонованого доступу, зокрема атак, що ґрунтуються на операціях перехоплення та вимірювання сигналів. Спроба несанкціонованого доступу до інформаційного потоку неминуче змінює фізичні параметри квантового середовища через вимірювання стану фотонів, що робить такі атаки виявленими. Хоча існують методи створення клонів фотонних потоків, їх повна ідентичність з оригіналом на даний момент є недосяжною, що підсилює надійність квантово-захищених систем передачі інформації [37 - 42].

Для організації систем підтримки прийняття рішень у квантово-механічних системах передачі інформації пропонується використання уніфікованих нейронних мереж. Такі мережі здатні автоматично аналізувати стан системи, класифікувати параметри та діагностувати стан інформаційних потоків, що дозволяє приймати обґрунтовані рішення щодо якості та надійності переданої інформації. Працюючи в режимі OLAP (Online Analytical Processing), така система може забезпечувати автоматичне управління процесом генерації та передачі інформації, реагуючи на критичні помилки або спроби несанкціонованого втручання без участі людини [55].

Ефект спостерігача, що виникає при вимірюванні стану фотона, призводить до його миттєвої зміни, що унеможливлює непомітне зчитування інформації. Таким чином, будь-яка спроба розпаралелювання фотонів викликає зміни, які стають очевидними при подальшому санкціонованому прийманні інформації [30-41].

Канал квантового зв’язку, що аналізується, складається з множини технологічних елементів, розподілених у просторі. Він функціонує у власному часі, який формується тактовими імпульсами, створюючи потік інформації. Така структура

забезпечує високий рівень захисту та ефективності передачі інформації у квантово-захищених системах.

У результаті аналізу інформаційних потоків у квантових каналах зв'язку (ККЗ) визначаються множини дискретних підмножин $i = 1, \dots, J$, що характеризують їх достовірність та функціональність. Аналіз включає встановлення стану цих підмножин та поточних характеристик, які відображають відповідність функціональних можливостей класам оцінки результатів роботи ККЗ. Досліджуваний канал зв'язку розбивається на підсистеми (блоки), кожна з яких складається з елементів системи зв'язку. Стан цих елементів (відмова або спрацьовування) однозначно визначає працездатність або відмову відповідних функцій, а також дозволяє ідентифікувати причинно-наслідкові зв'язки.

Завдання діагностики переважно належать до категорії класифікації, а іноді до кластеризації. Це впливає на архітектуру нейронної моделі, включаючи вибір функцій активації для різних шарів мережі, глибину та складність представлення вхідної інформації, а також методи інтерпретації результатів роботи нейронної мережі. Архітектура такої нейронної мережі може бути побудована на основі поєднання перцептронів Розенблата (рис. 2.1). Проблема вирішення логічних операцій типу XOR для перцептронів може бути успішно подолана за допомогою сигнатур алгебри Кантора для трьох логічних операцій: AND, OR, та NOT.

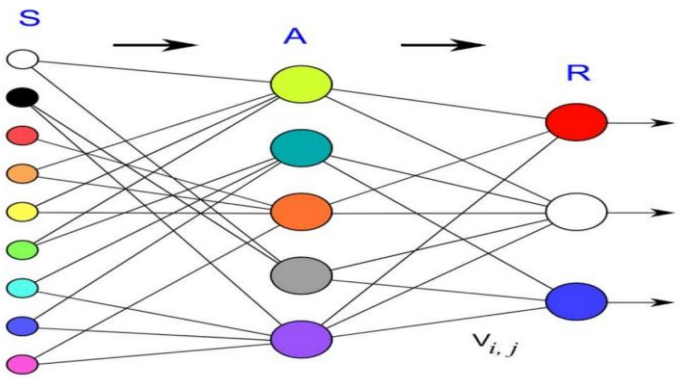


Рисунок 2.1 - Структура перцептрона Розенбата з проміжним асоціативним шаром

Вхідний шар мережі, що складається з множини симптомів *S*, забезпечує формування вихідних комбінацій незалежних та неантагоністичних проявів синдромів, які є зрозумілими для фахівців. Це дозволяє ефективно класифікувати сукупності поточних параметрів системи до рівня діагностики стану інформаційних потоків і зробити висновки щодо якості та надійності переданої інформації [57-60].

Таким чином, застосування нейронних мереж у процесах діагностики та класифікації стану квантових каналів зв’язку сприяє підвищенню точності та надійності систем підтримки прийняття рішень. Інтеграція методів машинного навчання з квантово-механічними аспектами забезпечує більш глибоке розуміння функціонування інформаційних систем та їх захисту від можливих загроз.

Проміжні шари нейронної мережі *A* відповідають за визначення множин станів ключових «сутностей» синдрому. Підсумкові синдроми формуються у вихідному шарі *R* і є конкатенацією цих сутностей. Фактично, це формула синдрому, яка складається з кон'юнкцій окремих сутностей, множина яких відображається на множині вихідних нейронів. Множина сутностей включає підмножини ключових визначників загальної формули синдрому.

Наприклад, гібридний синдром стану квантового каналу зв’язку (ККЗ) «ймовірна відмова третього розряду загального регістру з перетворенням інформації та можлива атака з перехватом фотонів регістру» є об'єднанням наступних сутностей: (відмова ∧ 3 розряд) ∪ (перетворення інформації ∧ спін фотона змінено) ∪ (ймовірна атака ∧ перехоплення). Залежно від складності проблеми та прояву наборів симптомів, синдром може бути гібридним і поєднувати ряд окремих синдромів. Такий підхід дозволяє детальніше аналізувати та класифікувати різні стани системи, забезпечуючи більш точну діагностику та ефективне управління інформаційними потоками в квантових каналах зв’язку [57].

Розробка імітаційної динамічної моделі (ІДМ) досліджуваного квантового каналу зв’язку здійснюється на відміну від відомих методів дискретно-подієвого моделювання за рахунок формалізованого опису причинно-наслідкових зв’язків між

стохастичними подіями та детермінованими процесами, що можуть виникати в каналах передачі інформації. Імітаційна модель, розроблена в рамках цього дослідження, дозволяє аналізувати сукупності сполучень подій і процесів, що відповідають цим сполученням за ланцюгами причинно-наслідкових зв'язків. Це забезпечує глибше розуміння динаміки роботи ККЗ та сприяє оптимізації її функціонування.

Вхідною інформацією для діагностики є множина k векторів симптомів $S = \bigcup_{j=1}^{k}(\bigcap_{m=1}^{n})_j$, де $s_i \in S$ належить до вхідного шару. Ця множина включає підмножини ієрархічних атрибутів, структурованих у деревоподібній формі з використанням мови структурованої розмітки XML. Вкладена ієрархічна структура дозволяє встановлювати відношення кожного симптому (листка дерева) до його локалізації прояву, приналежності до певного типу симптому, а також визначати вагові характеристики, що враховують інтенсивність та достовірність його прояву.

Безліч відображень елементів вхідного шару s_i на множини проміжного шару нейронів ak зважується значенням w_i. Сума зважених вхідних елементів визначає стан Ns_k k-го нейрону проміжного шару.

$$Ns_k = \sum_{i=0}^{n}(s_i \cdot w_i)_k, \tag{2.1}$$

При цьому функція активації, що визначає вихідне значення нейрона на виході проміжного шару, може відрізнятися від функції активації вихідного шару.

$$Na_r = \sum_{j=0}^{m}\left(s_j \cdot w_j\right)_r, \tag{2.2}$$

Стан нейрона використовується як аргумент для функції активації. Оскільки на вихідному шарі завершується процес визначення результатів класифікаційних

завдань, для функції активації $FR(N_{ar})$ доцільно використовувати функцію Leaky ReLU. Ця шматково-лінійна функція є диференційованою в діапазоні ймовірності кінцевого синдрому від нуля до одиниці та не викликає проблем у класифікаційних задачах. Для проміжних шарів функція активації $FA(N_{sk})$ має бути іншою. Автори досліджували ряд функцій активації та можуть запропонувати оригінальний варіант з нормованим діапазоном значень ваг [0;1] [58-60].

$$P(x) = \left(\frac{1}{\sqrt{2\pi}} \cdot \int_{0}^{6x-3} \exp\left(\frac{-t^2}{2}\right) dt \right) + 0.5, \tag{2.3}$$

На рисунку 2.2 показаний графік запропонованої функції активації FA~P(x) (x ∈ [0: 1]) – нормуючий параметр для проміжного шару нейронів).

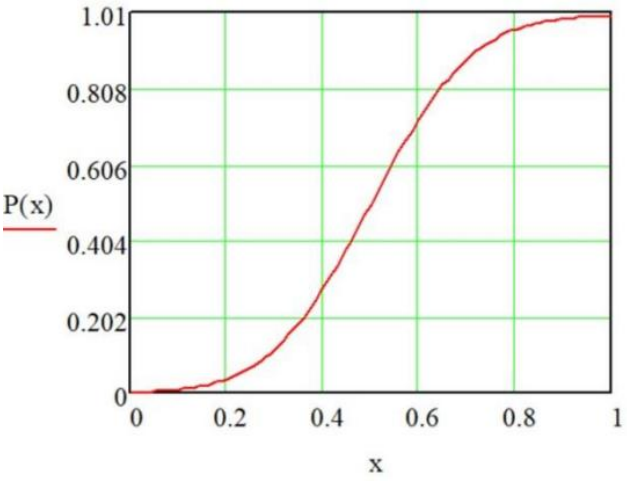


Рисунок 2.2 - Нормована функція активації

Запропонована архітектура нейронної мережі може бути використана в будь-яких класифікаційних задачах діагностики. Перш ніж використовувати таку структуру, необхідно провести початкове навчання мережі. Таке навчання за

ефективного інтерфейсу може проводитися не програмістом і навіть висококваліфікованим фахівцем у сфері діагностики.

Для створення та заповнення бази знань про синдроми необхідно мати мінімальний початковий набір безлічі кінцевих синдромів, кожен з яких є відображенням перетину сутностей формул синдрому, що відноситься до колекції проміжних шарів.

Кон'юнкції значень сутностей, фрагментованих з формули відповідного їм синдрому, що мають вагу зв'язку замовченням рівним 13, у міру заповнення бази знань корелюються. Значення колекції проміжних сутностей визначаються своєю чергою кон'юнкціями сукупностей симптомів.

Сукупність зв'язків наборів симптомів S_i сутності P_j і далі з синдромами зважується відносинами, надалі представленими як події e_{ij}.

$$\begin{array}{c} \\ P_1 \\ P_2 \\ \dots \\ P_m \end{array} \begin{array}{c} \begin{array}{cccc} S_1 & S_2 & \dots & S_n \end{array} \\ \begin{pmatrix} e_{11} & e_{12} & \cdots & e_{1n} \\ e_{21} & e_{22} & \dots & e_{2n} \\ \dots & \dots & \dots & \dots \\ e_{m1} & e_{m2} & \cdots & e_{mn} \end{pmatrix} \end{array} \tag{2.4}$$

де P_i – відображає ймовірність настання події e_{ij}.

Зв'язки елементарних подій відображені на їх ваги ймовірностей $e_{ij} \to p_{ij}, p_{ij} \in P_i$.

Навчання нейронної мережі проводиться безпосередньо експертом під час створення та наповнення бази знань. Налаштування нейронів здійснюється у зворотному порядку, починаючи з побудови множин синдромів R, векторів підмножин "сутностей" A, та векторів безлічі симптомів S.

По суті, результативна база знань є послідовним суб'єктивним відображенням функцій: $fA: S \to A$; $FR: A \to R$. Під час навчання використовується відомий метод зворотного проходження помилки. При цьому функція активації шару A, що добре диференціюється, дозволяє використовувати швидкий метод градієнтного спуску,

минаючи проблеми локальних мінімумів. Корекція ваг визначається за формулою [55]:

$$w_j(m+1) = w_j(m) - u \propto, \tag{2.5}$$

де u – коефіцієнт значимості алгоритму; $\propto$ – відхилення помилки.

У процесі навчання нейронної мережі експерт формує обмежену кількість векторів симптомів, встановлюючи при цьому симптоми антагоністи. Кожному створеному вектору ставить у відповідність результуючий вектор сутностей і відповідність правильному синдрому.

Оскільки жодних категорій значущості окремим симптомом не присвоюється при наповненні даних із різних джерел може виникнути проблема недостовірності. Надалі ми розглянемо її окремо. Навчання та корекція ваг проводяться паралельно при створенні кожного нового зв'язку і кожного нового синдрому. Це може призвести до проблеми динамічної зміни бази знань.

Проблеми конструювання нейронних моделей у діагностиці та пропозиції щодо їх подолання.

Методи діагностики що розглянуті в цій роботі спираються на недетерміновані моделі та дані про об'єкти діагностики, що призводить до низки проблем.

Проблема розмиття знань. Для системи діагностики використовують дані, отримані з різних джерел. Це теоретично дозволяє внести до бази знань суперечливі діагнози. Можуть виникнути алогізми, які неможливо знайти ніякими способами, крім втручання експерта. При створенні баз знань можуть виникнути проблеми достовірності знань, що вносяться. Так як будь-які елементарні симптоми є рівноважними та взаємно незалежними, то різні вектори симптомів для однакових синдромів отриманих з різних джерел (від різних авторів) можуть стати причиною відхилення від істинних значень даних синдромів (так званого розмиття знань). Для ефективного пошуку таких ситуацій пропонується використовувати кількісний показник, що визначається як сукупну частку вектора симптомів у багатьох формулах

діагностики. Підсумкова ймовірність достовірності вектора симптомів визначається за логічним АБО та показує частоту повторень для синдромів одного типу. При цьому якщо підсумкова частка сукупного вектора симптомів виявиться меншою, наприклад, ніж 0.90, можна припустити, що цей сценарій може мати ймовірність помилки 10 відсотків. Однак потрібно враховувати, що це лише середньостатистичний показник і не завжди може відповідати рівню достовірності синдрому, що розглядається.

Можлива ситуація коли одному й тому вектору симптомів відповідатимуть різні кінцеві синдроми. Це проблема виключного АБО.

Важливо, що цей алогізм не може бути усунений жодними способами, крім рішення експерта. Програмні засоби реалізують бази знань, що розглядаються, повинні бути забезпечені функціями пошуку проблеми XOR і не допускати одночасного використання суперечливих висловлювань. Динамічні зміни у базі знань. У міру заповнення бази знань, вагові коефіцієнти та вектори відображень змінюються, змінюючи також і логіку знань, що призводить до проблеми динамічних змін даних. Говорячи простою мовою, висновки мережі можуть суттєво змінюватися з процесом наповнення бази знань. Змінюватися до невпізнання. Це може впливати на сприйняття достовірності діагностики. Крім того, можна використовувати для побудови цілісних даних тільки реляційні бази даних, оскільки хронологія сховища даних не допускає змін у часі.

Вагові коефіцієнти нейронних зв'язків у мережі корелюються під час навчання мережі методом зворотного проходження помилок. Автори пропонують встановити початкові вагові значення коефіцієнтів лише на рівні 0,5. На першому кроці машинного навчання при встановленні зв'язку між вектором симптомів та підсумковим синдромом проводити операцію попередньої корекції ваг. Значення ваг w_j може набувати значення в діапазоні від [0; 1]. При цьому початкова кореляція ваги відповідає частоті його прояви в результативному синдромі для різних джерел інформації. Для синдрому, отриманого з єдиного джерела інформації, частота прояви зв'язку дорівнює одиниці. Достовірність інформації у разі не може бути визначена [60-62].

Для усунення такої невизначеності формулювання такого синдрому, необхідно вручну регулювати значення u ∝.

Достовірність навчання нейронної мережі. Антагонізм синдромів. Якщо розглядати синдром як відображення векторів симптомів на безліч синдромів, вважаючи таке відображення висловлюванням, то немає заборони на логічне протиріччя між висловлюваннями про один і той же синдром різними авторами. Виникає проблема антагонізму висловлювань.

Так як будь-яке висловлювання крім семантичного сприйняття несе також глибокий логічний сенс і є по суті знанням про модель діагностування, немає математичних способів виявити подібні алогізми. У такій ситуації одному й тому вектору симптомів ставляться у відповідність різні (можливо суперечливі) формули синдромів. Виникає проблема OR чи XOR. При цьому завданням системи підтримки прийняття рішень є пошук таких ситуацій та пропозиції корекції експерту.

На рисунку 2.3 представлена схема імітації роботи підконтрольного каналу зв’язку.

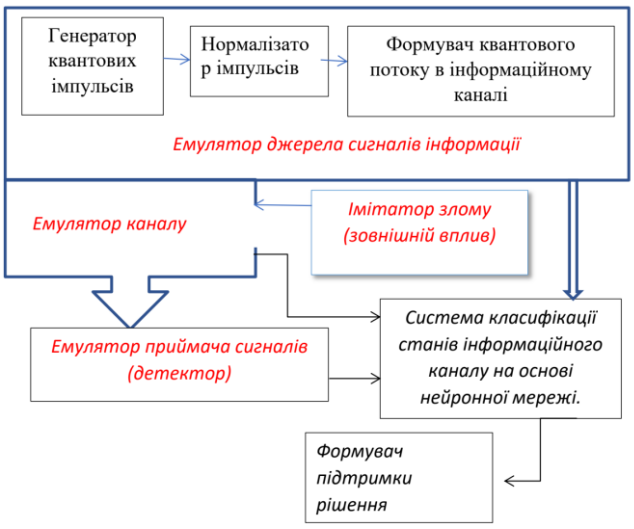


Рисунок 2.3 – Структурна схема роботи імітаційної динамічної моделі ККЗ

Емулятор приймача сигналів забезпечує формування множини станів регістрів каналу зв'язку у форматі, який дозволяє відобразити ці стани на інформаційну

множину вхідних нейронів системи класифікації стану інформаційного каналу. В свою чергу, вона програмно реалізує структуру нейронної мережі, яка має: шар вхідних нейронів; проміжний шар нейронів для формування патернів типових станів; вихідний шар нейронів, який відображає класи в стані при атаках або небажаних перетвореннях інформації.

Метою роботи цього програмного модуля є діагностика каналу зв'язку з подальшим відображенням даних, отриманих класифікатором, на множину рекомендацій або рішень модуля формування підтримки рішень.

Для формувач підтримки рішень розробляє уніфіковані протоколи управління пристроєм передачі даних. У протоколах регламентується послідовність та критичні значення атрибутів та показників інформаційної системи, на які формується однозначна реакція. Вважається, що інформаційна ємність пропонованої системи підтримки прийняття рішень не перевищуватиме 100 типових алгоритмів стратегій атаки та стільки ж небажаних впливів перетворення інформації.

Передбачається, що синхронізація та тривалість процесів інтелектуальної обробки інформаційних потоків не перевищуватимуть 50 мілісекунд на розряд каналу зв'язку. Таким чином, для восьмирозрядного каналу реакція системи підтримки рішень регламентується від 400 мілісекунд до 1 секунди. Такі показники можуть не задовольнити багатьох передбачуваних користувачів. Однак перспектива значного прискорення роботи нейронної мережі дуже обнадійлива і є предметом подальших досліджень.

2.2 Інформаційна модель інтелектуального аналізу стану системи квантової передачі інформації

Найчастіше використовуються когерентні атаки. При цьому зловмисники перехоплюють потік фотонів, зчитують дані у випадковому базисі та застосовують перебір порівняння інформації. Якщо базис побітного порівняння вгадано, то зловмисник генерує відповідний клоновий потік фотонів, надсилаючи його офіційному приймачу. Когерентність забезпечується збігом фаз перехоплених фотонів та згенерованих, відправлених офіційному приймачу.

Розмір ключа, який використовується для шифрування, впливає на ефективність захисту, зменшуючи ймовірність злому коду зі збільшенням розміру ключа N. Якщо проводити побітне порівняння відправлених та прийнятих фотонів для n-бітів, то ймовірність виявлення зловмисника, який міг перехопити частину цих бітів, дорівнює: $1 - 0.75^N$. Зазвичай з такими завданнями успішно справляється протокол BB84. При колективних атаках кожен фотон, отриманий від передавача, переплутується з фотонами, отриманими з квантових зразків. В результаті квантової заплутаності та побітного порівняння інформації зловмисник може визначити повний базис відправника. Якщо атака не є когерентною, то хакеру потрібно порівнювати кожен отриманий фотон у режимі перехоплення інформації та відправлення її клону.

Квантова заплутаність фотонів може бути забезпечена несепарабельним станом системи. Якщо 2-кубітна квантова система (для кубітів A і B) представлена вектором $|\varphi\rangle \in C^4 = C^2 \otimes C^2$, то цей стан називається сепарабельним (не заплутаним), якщо виконується рівність $|\varphi\rangle = |\varphi 1\rangle \otimes |\varphi 2\rangle$ для існуючих станів $|\varphi 1\rangle \in C^2$ кубіта A і $|\varphi 2\rangle \in C^2$ кубіта B. В іншому випадку, цей стан є несепарабельним (заплутаним) [5-6].

Використання властивості заплутаності фотонів в лініях передачі інформації може допомогти вирішити задачу непрозорих атак, у випадку перехоплення фотонів зловмисниками та відправки далі на приймач клонів таких заплутаних фотонів.

Приклад спроби застосування прозорої атаки для заплутаних фотонів приведено в таблиці 2.1.

Таблиця 2.1 - Приклад прозорої атака

Відправник	Випадковий біт	0	1	0	0
	Базис	+	×	×	×
	Поляризація	↑	↘	↗	↗
Хакер	Базис	+	+	+	×
	Поляризація	↑	→	→	↗
Отримувач	Базис	+	↗	↗	↗
	Поляризація	↑	↗	↗	↗
Ключ	Спотворення	-	+	-	-
	Витік	+	-	-	-

Окрім вказаних прикладів, можливі атаки з осліпленням однофотонного детектора, при яких кіберзлочинець зчитує інформацію передавача і відправляє її далі за допомогою дуже потужного імпульсу лазера. Такий прийом може призвести до того, що неідеальний детектор приймача сприймає імпульс без урахування ефекту спостерігача. В такому випадку зчитування інформації доступне без санкції. Якщо встановити перед детекторами випадкове джерело одиничних фотонів, то виникає можливість переконатися, що детектор не зчитує світлові сигнали, а працює в квантовому режимі. Тобто за рахунок виявлення квантових ефектів можливе виявлення кіберзламу [7-8].

Цікавий метод атаки з розділенням фотонів. За один такт передачі інформації може бути згенеровано кілька фотонів. Зазвичай генеруються лазерні світлодіоди малої потужності. Якщо виявиться, що фотонів більше двох, то хакер може спробувати розділити їх. І таким чином виникає заплутаність з пробним фотоном. Незмінна частина даних передається отримувачу, а зловмисник має можливість отримати правильне значення переданого біта, не вносячи додаткових похибок у

ключі при фільтрації. Це дозволяє залишатися непоміченим і перехоплювати інформацію [9-10]. Вирішення проблем такої атаки можливе за допомогою різних методів.

В даний час успішно ведеться розробка ідеальних джерел квантів з точно заданою кількістю генерації на один такт і абсолютно схожими характеристиками фотонів необхідної потужності. Крім того, вдосконалюються протоколи, такі як BB84 або SARG04 [11-13].

Окрім описаних варіантів, існує багато ситуацій реалізації унікальних атак або процесів перетворення інформації. Також необхідно враховувати, що можуть бути розроблені методи кіберзлому, які на даний момент не існують. Наразі відомо близько 20 типів таких атак, і кожного року їх кількість зростає приблизно на 20 відсотків. Для квантової передачі інформації використовуються складні електронно-оптичні пристрої.

Приховані та явні недоліки таких пристроїв також можуть представляти суттєву проблему для надійності та безпеки роботи квантових систем передачі інформації. У зв'язку з цим виникає завдання розробки та впровадження методів детектування перетворення інформації або несанкціонованого доступу до неї, ідентифікації та класифікації в квантових лініях зв'язку, створення інформаційних технологій якісної підтримки прийняття рішень в автоматичному режимі щодо процесів передачі інформації. Автори вважають, що одним з шляхів вирішення цих проблем може бути розробка технології інтелектуального аналізу даних на основі нейронних мереж, які могли б у режимі OLAP впоратися з класифікацією станів квантових потоків в реальному часі та забезпечити надійність та конфіденційність передачі цифрової інформації в квантовому режимі [55-57].

Квантовий стан готується макроскопічними пристроями. Змінюючи параметри пристрою, ми змінюємо параметри стану, і таким чином отримуємо можливість записувати класичну інформацію в квантовому стані. Найпростіший квантовий канал зв'язку математично задається сімейством (вихідних чи сигнальних) станів Sx де параметр x пробігає вхідний алфавіт. Відображення x → Sx у стиснутій формі містить

опис фізичного процесу, що породжує стан Sx. Наприклад, нехай x = 0, 1, причому S1 – когерентний стан поля випромінювання лазера, а S0 – вакуумний стан. В цьому разі ми маємо канал із двома чистими неортогональними станами.

Для того щоб отримати класичну інформацію, що міститься в квантовому стані, необхідно провести вимірювання. У наведеному вище прикладі таку роль відіграє будь-який приймач лазерного випромінювання з можливою подальшою обробкою результатів виміру. Якщо вимір задається базисом $|ey\rangle$, то умовна можливість отримати результат y, за умови, що був надісланий сигнал x, дається формулою $P(\text{y}|\text{x}) = (\text{e}y|\ Sx\ |ey\rangle$.

Таким чином, для фіксованого виміру ми отримуємо звичайний канал зв'язку. Це дає можливість поставити питання про максимальну кількість класичної інформації, яка може бути передана по даному квантовому каналу зв'язку та про його пропускну здатність.

Пропускна здатність будь-якого квантового каналу обмежена зверху величиною log dim H, причому ця величина досягається для "ідеального" каналу, сигнальні стани якого утворені векторами о.н.б. (ортонормований базис) у просторі H, а вимір задається цим же о.н.б. Таким чином, розмірність гільбертового простору є мірою максимального інформаційного ресурсу квантової системи.

Важливу роль в захисті інформації мають криптографічні ключі. В даній роботі вони розглядаються разом з іншими ознаками надійності та достовірності передачі інформації. Створення та розподілення ключів виконується на основі типових протоколів. Деякі протоколи розглянемо з точки зору прийнятного використання в класифікації завдяки нейронним мережам.

Передбачається, що є два віддалені один від одного учасники A та B, яким потрібен загальний двійковий ключ, тобто. двійкова послідовність к = (к1, . . . , к_m) довжини m. Цей ключ учасники хотіли б використовувати для кодування та декодування своїх повідомлень, також являють собою двійкові послідовності довжини m, шляхом літерного застосування операції XOR: $yk = xk \oplus \kappa k, xk = yk \oplus \kappa k$. Тут $x = (x_1, \ldots, x_m)$ – кодується повідомлення, а $y = (y_1, \ldots, y_m)$ –

закодоване повідомлення, яке А пересилає В для наступного декодування. Такий спосіб кодування/декодування зветься шифр Вернама. Оскільки ключ має бути секретним, важливою проблемою є знаходження способу його передачі (розподілу) обом учасникам, при якому ключ не може бути перехоплений або пошкоджений. Квантова криптографія пропонує такі способи (протоколи), надійність яких може бути в принципі як завгодно висока і забезпечується закономірностями квантової інформатики, такими як неможливість клонування квантового стану та додатковість між квантовим виміром і обуренням стану. Усі викладені нижче протоколи використовують те що, що стани $|0\rangle$, $|1\rangle$ збурюються при вимірі в базисі $\{|+\rangle, |-\rangle\}$, точніше, з ймовірністю 1/2 переходять у стани $|+\rangle$ або $|-\rangle$, і навпаки, стану $|+\rangle$, $|-\rangle$ при вимірі в базисі $\{|0\rangle, |1\rangle\}$ переходять у стан цього базису.

2.3 Математична модель оцінки ймовірних відмов надійної роботи системи квантової передачі інформації

Узагальнена математична модель процесів контролю стану системи квантової передачі інформації та алгоритмів підтримки рішень може бути представлена кортежом:

$$GIQ = \langle PK, R, Qb, F(S), Kk, DSS \rangle, \quad (2.6)$$

де

$Pk = \{ pk_j \}$ - множина показників квантового каналу зв’язку;

R - множина регістрів канал зв'язку по розрядах;

Qb - Множина інформаційних елементів Q бітів, які формують стан фотонного середовища каналу зв'язку;

$F(S) = \{f(s_i)\}$ - Функція розробки прийняття рішення, як повне сюр'єктивне відображення множини симптомів S на множину рішень DSS;

Kk - множина показників квантового каналу зв'язку, що відповідає формуванню стану порозрядних елементів;

DSS - множина елементарних рішень, що формують алгоритми дій в системі підтримки прийняття рішень.

Передбачається, що відомі:

- детерміновані показники фізичних процесів, які можуть виникати в і- й підсистемі для j-х станів, що відображає вектор симптомів на вектор подій:

$$fe_{ij}: \overrightarrow{S_{ıJ}} \to \overrightarrow{\Phi_{ıJ}}, j = 1..J, \tag{2.7}$$

де:

j - (набір елементарних подій, що призводять до відмов в каналу);

$\overrightarrow{S_{ıJ}}$- вектор параметрів, що відповідає поточному стану і-й підсистеми;

$\overrightarrow{\Phi_{ıJ}}$ - вектор фазових змінних квантових процесів, які можуть виникнути в і-й підсистемі.

Розглядається узагальнена модель нештатної ситуації в ККЗ для аналізу і передбачення наслідків ВІДМОВ.

При моделюванні використовуються квантові коди, що виправляють помилки. При передачі інформації по каналу з шумом, а також при виконанні квантових операцій, бажано використовувати код, який був би стійкий щодо помилок. У класичному випадку принципова можливість такого кодування при швидкостях передачі, менших за пропускну здатність, випливає з теореми Шеннона. Однак ця теорема не дає конструктивного способу побудови перешкодостійкого коду, і практичному вирішенню цієї проблеми присвячена значна частина досліджень з теорії інформації, що становить теорію кодування.

Найпряміший спосіб застрахуватися від помилок полягає у повторенні повідомлень (що, звичайно, знижує швидкість передачі). Нехай в алфавіті є всього два символи 0, 1. Тоді припустимо , що ймовірність зміни одного біта в процесі передачі дорівнює малій величині p, так що ймовірність зміни двох бітів p2 зневажливо мала. Розглянемо код 0 → 00, 1 → 11. Хоча цей код і дозволяє виявити та виправити деякі помилки, він має істотний недолік: наприклад, у ситуації однієї помилки у другому чи першому биті 00 → 01, 11→ 01 ми можемо сказати, яке повідомлення було закодовано. Але цього недоліку можна позбутися, якщо додати ще один розряд: 0 → 000, 1 → 111. Такий код буде вже на заваді стійким по відношенню до помилки в будь-якому одному біті, в тому сенсі, що зіпсовані слова, що виходять з 000 і 111, ніколи не збігаються і тому безпомилково помітні.

У квантовій статистиці безпомилкова помітність чистих станів (а ми тут матимемо справу тільки з ними) рівносильна ортогональності векторів станів. Прямолінійне узагальнення класичного рецепту повторення повідомлень на квантовий випадок наштовхується на труднощі – квантову інформацію неможливо розмножити. По суті квантової інформації, під час передачі через канал з помилками безпомилково повинні прийматися як базисні стани, та й усілякі їх суперпозиції |ψ . Таким чином, прямолінійне узагальнення коду повторення $|\psi\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle$ є нездійсненним. На перший погляд, завдання здається нерозв'язним, проте у роботах Шора і Стіна незалежно були побудовані перші приклади квантових кодів, які виправляють помилки.

Ідея полягає в наступному: є два віддалених один від одного учасники, A та B, які потребують спільний бінарний ключ, тобто послідовність $\kappa = (\kappa_1, \ldots, \kappa_m)$ довжини m. Цей ключ учасники бажають використовувати для кодування та декодування своїх повідомлень, які також є бінарними послідовностями довжини m, за допомогою операції XOR посимвольно: $y_k = x_k \oplus \kappa_k, x_k = y_k \oplus \kappa_k$. Тут $x = (x_1, \ldots, x_m)$ - повідомлення, яке кодується, а $y = (y_1, \ldots, y_m)$ - закодоване повідомлення, яке A відправляє B для подальшого декодування. Цей метод кодування/декодування відомий як шифр Вернама.

2.3.1 Протоколи розподілу секретного ключа

Оскільки ключ має бути секретним, важливою проблемою є знаходження способу його передачі (розподілу) обом учасникам, за якого ключ не може бути перехоплений або пошкоджений. Квантова криптографія пропонує такі способи (протоколи), надійність яких може бути в принципі як завгодно високою і забезпечується закономірностями квантової інформатики, такими як неможливість клонування квантового стану і додатковість між квантовим вимірюванням і збуренням стану.

Усі викладені нижче протоколи використовують той факт, що стани $|0\rangle$, $|1\rangle$ збурюються під час вимірювання в базисі $\{|+\rangle, |-\rangle\}$, точніше, з імовірністю 1/2 переходять у стани $|+\rangle$ або $|-\rangle$, і навпаки, стани $|+\rangle, |-\rangle$ під час вимірювання в базисі $\{|0\rangle, |1\rangle\}$ переходять у стани цього базису [8-18].

Протокол BB84. Протокол BB84, запропонований Беннетом і Брассаром можно модифікувати в наступні кроки:

1. Учасник А створює дві випадкові двійкові послідовності $a = (a_1, \dots, a_N), b = (b_1, \dots, b_N)$ довжиною $N = (4 + \delta)n, n \gg 1$, слід також враховуючи, що кожен біт a_k, b_l незалежні і мають розподіл $\{\frac{1}{2}, \frac{1}{2}\}$.

2. Учасник А створює чистий квантовий стан з вектором

$$|\varphi\rangle \oplus_{k=1}^{N} |\varphi_{a_k b_k}\rangle,$$

$$|\varphi_{00}\rangle = |0\rangle, \qquad |\varphi_{10}\rangle = |1\rangle$$

$$|\varphi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |\varphi_{01}\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

3. Учасник А надсилає цей стан учаснику В відкритим квантовим каналом. Якщо канал ідеальний (шум або стороннє втручання відсутні) то В отримує стан $|\psi\rangle\langle\psi|$, в іншому разі - збурений стан $E(|\psi\rangle\langle\psi|)$, де Е позначає дію каналу.

Учасник В генерує випадкову послідовність $b' = (b'_1, \ldots, b'_N)$ і на k-му кроці здійснює вимірювання в базисі $\{|0\rangle, |1\rangle\}$, якщо $b'_k = 0$, або в базисі $\{|+\rangle, |-\rangle\}$, якщо $b'_k = 1$. Результати його вимірювань утворюють двійкову послідовність $a' = (a'_1, \ldots, a'_N)$.

4. Учасник А надсилає послідовність b учаснику В через відкритий класичний канал. В порівнює b з b' і повідомляє А номери бітів, які співпадають ($b_k = b'_k$).

Якщо канал ідеальний, то для цих бітів з імовірністю 1 виконується $a_k = a'_k$, бо вимірювання проводили в базисі, що містить надісланий стан. З великою ймовірністю кількість таких бітів майже дорівнює половині від N, що дорівнює $(2 + \delta/2)n \geq 2n$. Якщо кількість співпадаючих бітів a і a' значно відрізняється від $2n$, це означає можливість стороннього втручання у квантовий канал передачі. Тому учасники А і В припиняють передачу і намагаються усунути можливість втручання.

5. А і В виконують тести, щоб визначити величину втручань через можливий шум або підслуховування. Для цього А випадково обирає n бітів відфільтрованого ключа і передає їхні значення (разом з номерами) учаснику В через відкритий канал. Імовірність отримати $\leq \nu_n$ помилок у цих n контрольних бітах і при цьому $\geq (\nu + \varepsilon)n$ помилок у решті бітів має порядок $exp[2O(\varepsilon^2 n)$. Тому за великих n можна вважати, що частка розбіжностей у цих секретних бітах, що залишилися, практично дорівнює ν. Якщо А і В виявляють, що ν перевершує деяке порогове значення ν_t, то вони вирішують, що було втручання і також припиняють цей раунд протоколу. Величина ν_t залежить від того, що відомо про можливості перехоплювача Е. У літературі наводять значення νt = 0.11 ÷ 0.25, залежно від виду атак перехоплювача і використовуваних засобів протидії.

6. Якщо встановлено, що $\nu < \nu_t$, то А і В здійснюють "узгодження інформації", щоб усунути неспівпадіння бітів і "підвищення конфіденційності" залишковими $\approx n$ бітами, щоб знищити інформацію, яку міг перехопити E під час попередніх відкритих операцій. При цьому дуже корисною є верхня квантова оцінка кількості інформації перехоплювача E. Останні операції відносяться до класичної інформатики. В результаті А і В отримують m n бітів спільного секретного ключа.

Уразі малих δ:

$$P\{2n \le (k: bk) = bk' \le (2+\delta)n) \ge 1 - 2exp\left[-\frac{1}{8}n\left(\delta^2 + o(\delta^2)\right)\right], \quad (2.8)$$

Вводячи біт розбіжності $\nu_k = b_k \oplus b'_k$, маємо $P\{\nu_k = 0\} = P\{\nu_k = 1\} = \frac{1}{2}$, $M_{\nu k} = \frac{1}{2}$. Ймовірність, що нас цікавить, дорівнює $(N = (4 + \delta)n)$

$$P\left\{2n \le \sum_{k=1}^{N} v_k \le (2+\delta)n\right\} = 1 - 2P\left\{\sum_{k=1}^{N}(v_k < 2n)\right\},$$

унаслідок симетрії розподілу суми щодо її математичного очікування $N/2 = (2 + \delta/2)n$, у такому разі

$$P\left\{\sum_{k=1}^{N} v_k < 2n\right\} = P\left\{\frac{1}{N}\sum_{k=1}^{N}(v_k - \frac{1}{2}) < -\varepsilon\right\}, \quad (2.9)$$

де $\epsilon = \frac{1}{2} - \frac{2n}{(4+\delta)n} = \frac{1}{8}(\delta + o(\delta))$.

Зауважимо, що при використанні нерівність Чебишева, під час доведення закону великих чисел, випливає

$$P\left(\left|\frac{1}{N}\sum_{k=1}^{N}(v_k - \frac{1}{2})\right| > \varepsilon\right) \le \frac{Dv_k}{N\epsilon^2} = \frac{1}{4N\varepsilon^2} \to 0$$

при N → ∞. Експоненціальна оцінка (2.8), набагато точніша за експоненціальну, випливає з нерівності Чернова:

$$P\left\{\frac{1}{N}\sum_{k=1}^{N}(v_k-\frac{1}{2})\le-\varepsilon\right\}=P\left\{\frac{1}{N}\sum_{k=1}^{N}(v_k-\frac{1}{2})\le-\varepsilon\right\}$$

$$\le exp\left[-2N\left(\varepsilon^2+(\varepsilon^2)\right)\right], \qquad (2.10)$$

Це витікає з наступного. Нехай $s\ >0$, тоді

$$P\left\{\frac{1}{N}\sum_{k=1}^{N}\left(v_k-\frac{1}{2}\right)\ge\varepsilon\right\}=P\left\{e^s\sum_{k=1}^{N}\left(v_k-\frac{1}{2}\right)\right\}\le e^{-sN\varepsilon}Me^s\sum_{k=1}^{N}\left(v_k-\frac{1}{2}\right)=$$

$$=e^{-sN\varepsilon}\left[s\left(v_k-\frac{1}{2}\right)\right]^N=e^{-sN\varepsilon}\left[cosh\left(\frac{S}{2}\right)\right]^N=e^{-N\left(s\varepsilon-lncosh\left(\frac{s}{2}\right)\right)}$$

При малих значеннях s

$$lncosh\frac{2}{s}=\frac{8^2}{s}+o(s^2)$$

З іншого боку,

$$max(s\varepsilon-\frac{s^2}{8})=2\varepsilon^2, s\ge0$$

до того ж максимум досягається для $s\ =\ 4\varepsilon$. Звідси отримуємо (2.10), а враховуючи, що $N\ =\ (4\ +\ \delta)n$.

Протокол B92. Протокол B92 реалізується наступними кроками:

1. Учасник A генерує випадкову двійкову послідовність $a\ =\ (a_1,\ldots,a_N)$ і на кожному кроці k створює чистий стан з вектором $|\psi_0\rangle\ =\ |0\rangle$, якщо $a_k\ =0$, або $|\psi_1\rangle=|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$, якщо $a_k\ =\ 1$.

2. Учасник A відправляє стан, задаючи вектором $|\varphi\rangle=\otimes_{k=1}^{N}|\varphi_{a_k}\rangle$, учаснику B по відкритому квантовому каналі. Учасник B генерує випадкову послідовність $a'=(a'_1,\ldots,a'_N)$ *yf k*-тому кроці виконує вимірювання у базісі $\{|0\rangle|1\rangle\}$ якщо $a'_k\ =\ 0$, або у

базіс $\{|+\rangle|-\rangle\}$, $a'_k = 1$. Східний плюс кодується як 0, мінус як 1. Таким чином результат вимірювання В утворює двійкову послідовність b=(b1,...,bN). Слід також зазначити, що $a_k = a'_k$ тоді $b_k = 0$, тому з $b_k = 1 \Rightarrow a_k \neq ak$, тобто $a_k = 1 - a'_k$.

3. Учасник В відправляє послідовність b учаснику А по відкритому класичному каналі. А (відповідно В) залишає тільки ті біти послідовності a (відповідно a'), для яких $b_k = 1$. Отримані таким чином таємні біти $a_k = 1 - a'_k$ складають відфільтрований ключ.

4. Наступні кроки аналогічні відповідним крокам протоколу BB84.

Протокол E91. Учасники А і В отримують «половинки» зчепленого стану $|\varphi\rangle = \otimes_{k=1}^{N} |\varphi_{a_k}\rangle$ де $|\varphi k\rangle = \frac{1}{\sqrt{2}}(|100\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$ де перший q-біт.

Учасник А генерує випадкову двійкову послідовність $a = (a_1, \ldots, a_N)$. На k-му кроці А проводить вимірювання в базисі $\{|0\rangle, |1\rangle\}$, якщо $a_k = 0$, або в базисі $\{|+\rangle, |-\rangle\}$, якщо $a_k = 1$, та отримує результати $a' = (a'_1, \ldots, a'_N)$.

Відповідно В генерує послідовність $b = (b_1, \ldots, b_N)$, вимірює в базисі, обраному за b_k, і отримує результати $b' = (b'_1, \ldots, b'_N)$.

З рівності (2.9) випливає, що якщо на k-му кроці А і В проводять вимірювання в однакових базисах: $\{|0\rangle, |1\rangle\}$ або $\{|+\rangle, |-\rangle\}$, то вони отримують співпадаючі результати, $P\{ak' = bk'\} = 1$.

Використовуючи відкритий класичний канал, А і В порівнюють a і b і залишають відфільтрований ключ тільки ті біти a' (відповідно b'), для яких $a_k = b_k$, тобто А і В використовували для k-го вимірювання однакові базиси. У цьому протоколі біти просіяного ключа $a'_k = b'_k$ не просто відбирають, але створюють під час вимірювань.

Описані вище протоколи реалізовано в експерименті, більше того, для перших двох створено комерційні зразки обладнання. Доведення їхньої стійкості є непростим завданням, яке вимагає залучення всього інструментарію квантової теорії інформації.

Учасник А генерує випадкову двійкову послідовність $a = (a_1, \ldots, a_N)$. На k-му кроці А проводить вимірювання в базисі $\{|0\rangle, |1\rangle\}$, якщо $a_k = 0$, або в базисі $\{|+\rangle, |-\rangle\}$, якщо $a_k = 1$, та отримує результати $a' = (a'_1, \ldots, a'_N)$.

Відповідно В генерує послідовність $b = (b_1, \ldots, b_N)$, вимірює в базисі, обраному за b_k, і отримує результати $b' = (b'_1, \ldots, b'_N)$.

З рівності (2.8) випливає, що якщо на k-му кроці А і В проводять вимірювання в однакових базисах: $\{|0\rangle, |1\rangle\}$ або $\{|+\rangle, |-\rangle\}$, то вони отримують співпадаючі результати, $P\{a'_k = b'_k\} = 1$.

Використовуючи відкритий класичний канал, А і В порівнюють a і b і залишають відфільтрований ключ тільки ті біти a' (відповідно b'), для яких $a_k = b_k$, тобто А і В використовували для k-го вимірювання однакові базиси. У цьому протоколі біти просіяного ключа $a'_k = b'_k$ не просто відбирають, але створюють під час вимірювань.

Описані вище протоколи реалізовано в експерименті; більше того, для перших двох створено комерційні зразки обладнання. Доведення їхньої стійкості є непростим завданням, яке вимагає залучення всього інструментарію квантової теорії інформації.

2.4 Імітаційна модель контролю квантового каналу зв'язку

Для розробки надійної системи класифікації стану лінії квантового передавання інформації пропонується створити емулятор, який зміг би віртуально уявити універсальну абстрактну систему генерації квантових сигналів, імітувати передачу квантової інформації у різних режимах, а також типові процеси спроб взлому лінії передачі квантової інформації. Розробити структуру нейронної мережі та математичний апарат обробки квантової інформації, яка змогла б підключатися до емулятора за допомогою універсального відкритого протоколу і виконувати завдання обробки віртуальної інформації в активному OLAP режимі. Необхідно також

розробити інформаційну модель та методи навчання і експлуатації нейронної мережі для чіткої та достовірної класифікації стану ліній передачі інформації з метою вироблення рекомендацій у системі підтримки прийняття рішень щодо забезпечення надійності та конфіденційності даних. Важливою задачею дослідження при цьому є визначення меж і характеристик роботи нейронної мережі, її можливостей обробки інформації в реальному часі, а також можливостей навчання на прикладах реальних ситуацій при обробці інформації. На рис. 2.3 представлена структура такої інформаційної системи СППР.

Емулятор джерела сигналів інформації забезпечує вхідний стан системи квантової передачі даних. Генератор квантових імпульсів імітує потоки фотонів, необхідних для формування q-бітів. Нормалізатор сигналів забезпечує заповнення множин вхідних станів, що відповідають процесу формування черги бітів за регістрами каналу зв'язку. Формувач квантового потоку в інформаційному каналі відповідає процесу модуляції або заповнення бітами цінної інформації, необхідної для передачі, а також формування ключів. В результаті емулятор джерела формує блок вхідної інформації каналу зв'язку та створює множини, що відображають атрибути q-бітів системи.

Емулятор каналу зв'язку переміщає потік бітів інформації між вхідними та вихідними регістрами, імітуючи процес проходження фотонів через оптоелектронні пристрої. При цьому програмні модулі блоку імітаторів злому або зовнішнього впливу та емулятора каналу зв'язку взаємодіють між собою, імітуючи зміну інформації у разі несанкціонованого доступу або небажаного зовнішнього впливу. Такі впливи формуються в програмному модулі імітації злому за алгоритмами, що відповідають стратегіям несанкціонованого доступу або атак, описаним вище. Програмне забезпечення цієї частини системи передбачає стандартний протокол представлення та введення даних за зовнішніми алгоритмами, створеними експертами в галузі кібербезпеки. Чим більше стратегій атаки буде розглянуто, тим більш досконалою буде розроблювана система підтримки прийняття рішень.

Емулятор приймача сигналів забезпечує формування множини станів регістрів каналу зв'язку у форматі, який дозволяє відобразити ці стани на інформаційну множину вхідних нейронів системи класифікації стану інформаційного каналу. В свою чергу, вона програмно реалізує структуру нейронної мережі, яка має шар вхідних нейронів, проміжний шар нейронів для формування патернів типових станів та вихідний шар нейронів, який відображає класи в стані при атаках або небажаних перетвореннях інформації. Метою роботи цього програмного модуля є діагностика каналу зв'язку з подальшим відображенням даних, отриманих класифікатором, на множину рекомендацій або рішень модуля формування підтримки рішень.

Для формувача підтримки рішень розробляються уніфіковані протоколи управління пристроєм передачі даних. У протоколах регламентується послідовність та критичні значення атрибутів та показників інформаційної системи, на які формується однозначна реакція. Вважається, що інформаційна ємність пропонованої системи підтримки прийняття рішень не перевищуватиме 100 типових алгоритмів стратегій атаки та стільки ж небажаних впливів перетворення інформації. Передбачається, що синхронізація та тривалість процесів інтелектуальної обробки інформаційних потоків не перевищуватимуть 50 мілісекунд на розряд каналу зв'язку. Таким чином, для вісьмирозрядного каналу реакція системи підтримки рішень регламентується від 400 мілісекунд до 1 секунди. Такі показники можуть не задовольнити багатьох передбачуваних користувачів. Однак перспектива значного прискорення роботи нейронної мережі дуже обнадійлива і є предметом подальших досліджень.

2.5 Побудова функціональної схеми інтелектуального аналізу каналу інформації на основі нейронної мережі

Процедури аналізу стану каналу зв'язку можуть розглядатися як процеси з чіткою логікою. Експерт, що використовує канал зв'язку на основі об'єктивних

показників так званих «симптомів» має можливість встановити причинно-наслідкові зв'язки між показниками симптомів, об'єднаних в множину поточних даних та «діагнозом» або синдромом для ККЗ і надалі прийняти послідовне прийняття рішення щодо управління каналом.

Результатом прийняття рішення може бути протокол управління ККЗ за точно встановленим сценарієм застосування впливів та заходів апаратного та інформаційного характеру, послідовності проведення процедур та других процесів.

На рис. 2.4 пропонується формалізована система нейронних ланцюгів, завдяки якій можна засобами дискретної математики описати знання процесів постановки діагнозу та прийняття рішення щодо управління каналом. Така структура нейронної мережі є базовою і можливо, що в процесі розробки потрібно додати деякі нейронні шари.

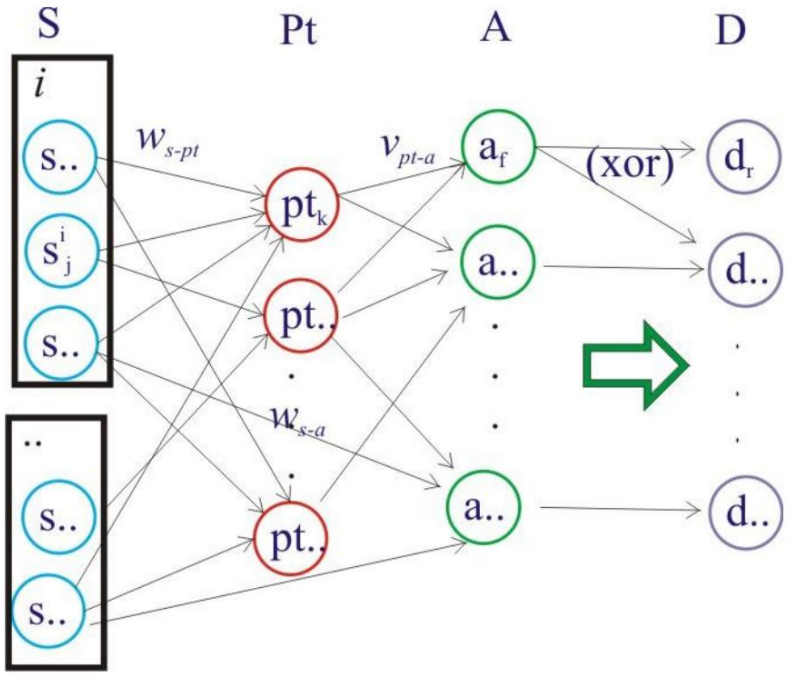


Рис. 2.4 Структура нейронної мережі ККЗ

Вхідний шар нейронів S розбитий на кластери за ознакою симптомів.

Шар нейронів патерн Pt. Патерн - це елементарні формули, об'єднання яких дають формулу синдрому в шарі A.

Сукупність груп симптомів відображається функціонально на патернах.

Зв'язки такого відображення зважуються вагою W.

Сукупності елементарних патерн відображаються на шарі синдрому (анамнез) A. По суті синдром - це діагноз, складений як формула з патерн і містить інформацію про стан ККЗ.

Наступний шар рішень D (decision) містить інформацію про ті заходи, які необхідно вжити для забезпечення надійної роботи ККЗ.

Таким чином, при занесенні даних формується дерево рішень. Вся структура при глибокому машинному навчанні представлятиме собою ліс рішень, які є узагальненням досвіду висококваліфікованого експерта, який проводить навчання нейронної мережі.

Подана структура є замкнутим графом станів, що враховують причинно-наслідкові зв'язки між вхідною інформацією симптомів та послідовністю процедур управління, описаних у шарі D.

Навчання нейронної мережі спочатку ґрунтується на описі існуючих та відомих процедур протоколів, представлених експертами криптографами.

При цьому методом зворотного поширення помилки коригується вага зв'язків усередині нейронної структури.

У міру внесення даних у селі рішень якість та надійність (імовірність успіху) зростає зі збільшенням вагових критеріїв. Настане момент, коли генерація нового раніше не внесеного синдрому та рішень для певної комбінації вхідних даних отримає вагову оцінку понад 95%. В цьому випадку можна припускати, що система навчена достатньо для її практичного застосування.

Система у поданому вигляді не є автоматичною, а є автоматизованою. Тобто кожне рішення надається оператору ККЗ як консиліум, але на його розсуд остаточний результат.

Все описана вище пропозиція вимагатиме створення програмного забезпечення, інтерфейсної частини, наповнення баз даних та бази знань, а також тестової частини отримання діагнозу та вироблення рішень з управління ККЗ.

Висновок до Розділу 2

У межах даного дослідження обґрунтовано та запропоновано модель інформаційної технології підтримки прийняття рішень для квантових систем передачі інформації, яка поєднує методи імітаційного моделювання, формальні математичні підходи та інструменти інтелектуального аналізу даних. Суттєвою науковою новизною роботи є інтеграція квантово-механічних принципів формування інформаційних потоків з архітектурою нейронних мереж, що дозволяє розглядати діагностику станів каналу як задачу багатовимірної класифікації. Основні матеріали розділу викладені в публікації [53, 54, 65].

РОЗДІЛ 3. МЕТОДИ СТАТИСТИЧНОГО ТА ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ В ІНФОРМАЦІЙНІЙ ТЕХНОЛОГІЇ ПІДТРИМКИ РІШЕНЬ ДЛЯ ЗАХИЩЕНОЇ СИСТЕМИ КВАНТОВОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ

У сучасних умовах забезпечення безпеки квантових комунікацій набуває особливої актуальності. Незважаючи на те, що квантова криптографія гарантує високий рівень захисту інформації, реальні експлуатаційні системи піддаються впливу численних факторів, що можуть свідчити про потенційні атаки. Отже, завдання дослідження полягає у розробці інтегрованої інформаційної технології, яка об’єднує статистичний аналіз, кластеризацію інтелект для оперативного виявлення аномалій у параметрах квантового каналу.

3.1 Інтеграція даних і параметричне обґрунтування безпеки квантовому розподілу криптографічного ключа

У даному дослідженні забезпечення безпеки квантового каналу зв’язку ґрунтується на комплексному аналізі фізичних та логічних параметрів, що відображають стан системи під час нормальної роботи та потенційних атак. Вибір конкретних величин: потужність лазерного випромінювання (P_{Laser}, мкВт); номер біту (Bit_{Number}); рівень шуму ($Noise$, Гц); співвідношення сигнал/шум (SNR, дБ); бітова помилка (Bit_{error}); час прибуття фотона ($T_{\mathrm{ArrivalTime}}$, рс); час детектування (T_{detect}, рс), час паузи (T_{paus}, рс) - не є випадковим, оскільки кожна з них надає унікальну інформацію про роботу каналу та його потенційні вразливості [65, 69].

Номер біту (Bit_{Number}) забезпечує часову послідовність отриманих даних, що є необхідною умовою для аналізу часових залежностей і виявлення групових аномалій

у роботі системи. Одночасно, індикатор помилки біту, який приймає значення 0 або 1 (відповідно, правильне або неправильне розпізнавання біту), є прямим показником якості передачі інформації. Статистичний аналіз співвідношення правильних і неправильних розпізнавань дозволяє оцінити ефективність каналу і виявити перші ознаки потенційних атак або апаратних збоїв.

Фізичні параметри, такі як, потужність імпульсу, рівень шуму, тривалість, співвідношення сигнал/шум, час детектування, складають ядро інформації про фізичний стан каналу. Поляризація, як ключовий параметр для квантових протоколів, дозволяє відстежувати, чи не відбулися зміни, які можуть бути спричинені як природними флуктуаціями, так і навмисним впливом з боку зловмисників. Показники потужності та тривалості імпульсу є важливими для оцінки співвідношення сигнал/шум, що прямо впливає на якість детектування сигналу. Аналіз часу детектування дозволяє виявити затримки у роботі системи, які можуть бути ознакою атак або апаратних несправностей, а параметр часу паузи є важливим для підтримки коректної синхронізації системи [66 – 70].

Крім того, рівень шуму, зумовлений особливостями оптичного волокна, відіграє важливу роль при оцінці фізичного стану каналу. Аналіз цього показника допомагає відокремити природні флуктуації від системних аномалій, що можуть бути спричинені зовнішніми впливами або атаками. Визначення базового рівня шуму є необхідним кроком для нормалізації інших параметрів і подальшої побудови кореляційних моделей [71-74].

Інтеграція зазначених параметрів дозволяє сформувати багатовимірний простір даних, у якому кожен вимір доповнює інший. Такий підхід сприяє комплексному аналізу, оскільки дає можливість не лише досліджувати окремі показники, але й встановлювати взаємозв’язки між ними. Наприклад, можна виявити, що збільшення кількості помилок тісно пов’язане із зростанням рівня шуму або змінами у часі пауз, що дозволяє створити індикатори аномалій, які використовуються як вхідні дані для алгоритмів класифікації та кластеризації [75, 76].

Таким чином, інтеграція вихідних параметрів у загальну методологію дослідження створює міцну основу для побудови адаптивної системи моніторингу квантового каналу. Використання комплексного підходу, що поєднує фізичні показники (P_{Laser}, T_{imp}, T_{detect}, T_{paus}, $T_{ArrivalTime}$, $Noise$) із логічними параметрами (Bit_{Number} і Bit_{Error}), забезпечує можливість оперативно виявляти відхилення від нормальної роботи, своєчасно реагувати на потенційні загрози і підтримувати високу якість передачі даних [71, 72].

Це, в свою чергу, є запорукою підвищення рівня безпеки в умовах сучасних квантових комунікацій і дозволяє розробити систему підтримки рішень, яка здатна адаптуватися до змін у роботі каналу та ефективно протидіяти зовнішнім загрозам.

3.2 Оцінка статистичних показників параметрів дослідження

Методика розрахунку статистичних показників ґрунтується на застосуванні класичних математичних формул, що широко використовуються у сфері інформаційних технологій та системного аналізу. Арифметичне середнє, яке є мірою центральної тенденції [79, 80]:

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{3.1}$$

де N - кількість вимірювань; x_i - значення i-го параметру.

Цей показник дозволяє встановити базовий рівень роботи квантового каналу в умовах нормального режиму, що є важливим для порівняльного аналізу з експериментальними даними.

Стандартне відхилення розраховується за наступною формулою:

$$\sigma = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})^2}, \quad (3.2)$$

Дозволяє кількісно оцінити ступінь розсіяння виміряних даних навколо середнього значення. Значення стандартного відхилення є критерієм стабільності параметру: чим воно більше, тим більша варіативність у вимірюваних значеннях, що може свідчити про нестабільність роботи каналу або вплив зовнішніх чинників [69].

Медіана $\tilde{x}$ визначається як середнє значення впорядкованої послідовності даних. При нечітко заданих математичних формулах для медіани зазвичай використовується алгоритмічний підхід [81]:

- якщо N непарне, медіаною є значення, яке знаходиться посередині впорядкованої послідовності;

- якщо N парне, медіаною вважають середнє арифметичне двох центральних значень.

Інтервал значень Δx, визначений як різниця між максимальним та мінімальним значенням і дозволяє оцінити загальний розкид вимірювань.

$$\Delta x = x_{max} - x_{min}, \quad (3.3)$$

Додатково, коефіцієнт варіації (CV) розраховується як відношення стандартного відхилення до середнього значення, виражене у відсотках:

$$CV = \left(\frac{S}{\bar{x}}\right) \times 100\%, \quad (3.4)$$

є відносною мірою розсіяння даних і дозволяє порівнювати варіативність параметрів незалежно від їх абсолютного масштабу. Використання коефіцієнта

варіації є надзвичайно корисним у контексті інформаційних технологій, де різні параметри можуть мати суттєво відмінні порядки величин [77].

Інтеграція отриманих даних із загальною системною архітектурою дозволяє розробити адаптивну систему підтримки прийняття рішень. На основі побудованих статистичних моделей, що враховують середні значення, стандартні відхилення та коефіцієнти варіації, система може автоматично відслідковувати відхилення від нормальних режимів роботи. Наприклад, відхилення значень параметрів на більше ніж 3σ від середнього можуть розглядатися як сигнал для ініціювання профілактичних заходів або для додаткової діагностики апаратного забезпечення [79].

Крім того, отримані дані використовуються як вхідні ознаки для алгоритмів класифікації та машинного навчання, зокрема для тренування нейронних мереж, що забезпечують прогнозування появи аномалій у режимі реального часу. Таким чином, комплексний аналіз статистичних характеристик не лише дозволяє об’єктивно оцінити поточний стан квантового каналу, але й інтегрується у систему підтримки прийняття рішень, що сприяє підвищенню безпеки та стабільності сучасних інформаційних систем.

Після узагальненого аналізу інтегрованих статистичних показників, доцільно перейти до детального розгляду даних за окремими режимами роботи каналу (стаціонарний режим роботи каналу передачі та аномальний). Такий підхід дозволяє не лише краще зрозуміти поведінку квантового каналу в режимі нормальної експлуатації, але й виявити особливості його роботи в умовах потенційних атак чи експериментальних змін.

У стаціонарному режимі роботи каналу зв’язку було проведено статистичний аналіз ключових параметрів, що характеризують фізичний стан каналу та якість квантової передачі інформації. Метою цього аналізу є визначення ступеня стабільності системи, оцінка ризику появи помилок, а також виявлення можливих факторів, що впливають на достовірність квантового обміну, таблиця 3.1.

Таблиця 3.1 - Статистичні характеристики фізичних параметрів квантового каналу в стаціонарному та аномальному режимах

Параметр	$\bar{x}$	σ	Δx	CV(%)	QBER(%)
Стаціонарний режим роботи каналу зв'язку					
P_{laser}	0,130	0,001	0,009	0,769	6
$Noise$	899,998	3,002	25,900	0,334	
$T_{ArrivalTime}$	0,125	49,975	42,312	0,476	
T_{imp}	99,994	0,999	9,213	0,999	
T_{detect}	1500,019	20,077	184,805	1,338	
Аномальний режим роботи каналу зв'язку					
P_{laser}	0,128	0,003	0,020	2,337	17
$Noise$	934,984	19,666	146,765	2,103	
$T_{ArrivalTime}$	124,876	114,443	895,466	91,645	
T_{imp}	106,513	3,658	36,578	3,434	
T_{detect}	1600,006	71,293	557,743	4,456	

Середньоквадратичне відхилення потужності лазерного випромінювання P_{laser} становить лише 0,001 мкВт при середньому значенні 0,130 мкВт, що свідчить про виключно високу стабільність джерела випромінювання. Коефіцієнт варіації, який дорівнює 0,769%, додатково підтверджує, що відхилення потужності не перевищує одного відсотка від середнього рівня. Це є критично важливою умовою для забезпечення однозначного кодування квантових станів у протоколі BB84, де використовується слабке когерентне випромінювання. При цьому рівень квантової бітової похибки (QBER) перебуває на рівні 6%, що цілком узгоджується з теоретично допустимими значеннями для стаціонарного режиму роботи каналу.

Дуже низьким виявився рівень флуктуацій шуму - середнє значення 900 Гц супроводжується стандартним відхиленням лише 3 Гц, а коефіцієнт варіації не перевищує 0,34%. Це дає підстави стверджувати, що фоновий шум системи добре контрольований і не чинить істотного впливу на надійність прийому квантових

сигналів. Висока стабільність шумових характеристик є ознакою ефективного екранування та мінімального впливу навколишнього середовища на оптичну систему.

Водночас параметр «час прибуття фотонів» виявився значно менш стабільним. Хоча середнє значення часу прибуття становить лише 0,125 нс, стандартне відхилення досягає 49,975 нс, а розмах перевищує 442 нс. Це свідчить про наявність окремих випадків з великою затримкою фотонів, що, однак, не супроводжується зростанням QBER і, відповідно, не є ознакою атаки типу затримки чи зміни поляризації. Ймовірною причиною такої поведінки є природні статистичні флуктуації в межах квантових процесів детекції.

Інші параметри - зокрема тривалість імпульсу та час детекції - продемонстрували високий рівень повторюваності та симетричність розподілу. Так, середнє та медіанне значення T_{imp} збігаються, стандартне відхилення не перевищує 1 мкс, а коефіцієнт варіації знаходиться на рівні 1%. Параметр T_{detect} виявився дещо варіативнішим, але в межах прийнятної норми, з CV близько 1,34%. Це свідчить про те, що обробка сигналів приймачем здійснюється стабільно, а фотоелектронна система функціонує без критичних збоїв.

Таким чином, узагальнюючи результати аналізу, можна стверджувати, що у стаціонарному режимі канал зв’язку демонструє високий рівень стабільності, контрольованості фізичних параметрів та відповідності характеристик технічним нормам. Відсутність різких відхилень або зростання рівня помилок свідчить про те, що система перебуває у штатному режимі, без впливу зовнішніх атак чи нестандартних подій. Це забезпечує надійну основу для безпечного квантового розподілу ключів.

У аномальному режимі роботи квантового каналу зв’язку було зафіксовано суттєве зростання коливань більшості досліджуваних параметрів, що може свідчити про зміну умов передачі, порушення стабільності каналу або можливий вплив зовнішніх факторів. Проведений статистичний аналіз дозволяє зробити низку висновків щодо характеру цих змін та їх потенційного впливу на надійність квантової комунікації.

Потужність лазерного випромінювання, яка у стаціонарному режимі залишалась майже незмінною, у аномальному середовищі виявляє більшу варіативність. Середнє значення дещо зменшилось до 0.128 мкВт, а стандартне відхилення зросло до 0.003 мкВт. Розмах значень також збільшився більш ніж удвічі порівняно зі стаціонарним режимом. Коефіцієнт варіації зріс до 2.337%, що вказує на зниження стабільності лазерного джерела. Особливо тривожним є підвищення рівня квантової бітової похибки до 17%, що суттєво перевищує поріг безпечної роботи та прямо вказує на потенційні втручання або критичні збої в оптичному тракті.

Рівень шуму в системі зріс як за середнім значенням (934.984 Гц), так і за дисперсією — стандартне відхилення сягнуло 19.666 Гц, що більш ніж у 6 разів перевищує відповідне значення в стаціонарному режимі. Розмах коливань також суттєво зріс і досягнув 146.765 Гц. Це свідчить про появу непередбачуваних шумових компонентів у каналі, які можуть бути спричинені як фізичними нестабільностями, так і зовнішнім втручанням, наприклад, неузгодженістю системи синхронізації.

Найбільш виразні зміни спостерігаються у часі прибуття фотонів. Середній час зростає до 124.876 нс, а стандартне відхилення збільшується до 114.443 нс. Медіана, яка раніше була близькою до середнього значення, тепер становить лише 111.665 нс, що свідчить про асиметрію розподілу. Розмах у 895.466 нс підтверджує наявність широкого діапазону затримок. Такі флуктуації можуть вказувати на дестабілізацію оптичного шляху, зміну рефракційних властивостей середовища або втручання сторонніх джерел, які змінюють фазові або часові характеристики квантових станів.

Сукупність отриманих даних демонструє, що у анамальному режимі канал зв’язку втрачає детерміновану структуру, а процеси, які у стаціонарному випадку мали нормальний або близький до симетричного розподіл, набувають аномальної дисперсії, асиметрії та загальної нестабільності. Такі ознаки є типовими маркерами наявності латентних аномалій або зовнішніх деструктивних впливів.

У зв’язку з виявленими відхиленнями у розподілах параметрів і появою ознак багатомодальності та асиметрії, особливо для параметрів $T_{ArrivalTime}$, $Noise$ та QBER, постає обґрунтована потреба у візуалізації розподілу вибірки через побудову

гістограм. Гістограма дозволяє наочно оцінити форму розподілу, наявність мод, асиметрію, «хвости» або інші аномалії, які не завжди очевидні з табличних статистик. Особливо важливим є виявлення відхилень від нормального розподілу, що може слугувати індикатором атак на канал або внутрішніх технічних збоїв. Таким чином, побудова гістограм є не лише допоміжним аналітичним інструментом, але й критично важливим етапом у верифікації гіпотез про зміну режиму роботи квантового каналу та виявлення потенційних загроз безпеці передачі [75- 79].

3.3 Використання Z-score для виявлення критичних станів у квантових системах підтримки рішень

Виявлення критичних відхилень у параметрах квантового каналу є однією з ключових задач інформаційних технологій підтримки рішень у квантових комунікаційних системах. Зміни фізичних характеристик каналу, таких як інтенсивність лазерного випромінювання, рівень шуму, співвідношення сигнал/шум або час прибуття фотонів, можуть бути наслідком як природних коливань, так і цілеспрямованих атак [82]. Ефективне виявлення таких змін вимагає використання швидких і надійних статистичних інструментів, здатних працювати в режимі реального часу.

Одним із найбільш поширених та ефективних методів є стандартизований показник Z-score, який визначає, на скільки стандартних відхилень S певне спостереження X відрізняється від середнього значення $\bar{x}$ у вибірці [83]. Його розрахунок виконується за формулою:

$$|Z| = \frac{X-\bar{x}}{\sigma}, \tag{3.5}$$

Цей підхід дозволяє уніфікувати параметри з різними масштабами та одиницями виміру, переводячи їх у спільну безрозмірну шкалу. У межах класичної інтерпретації вважається, що значення $|Z| \leq 2$ відповідають нормальному стану системи, значення у діапазоні $2 < |Z| \leq 3$ можуть свідчити про аномальні коливання, а $|Z| > 3$ - про критичний стан, що потребує негайного реагування [81-86].

Впровадження Z-score в архітектуру квантових систем підтримки рішень передбачає його використання на початковому етапі обробки вимірюваних даних. Після обчислення стандартизованих значень формується вектор ознак, який передається до модулів подальшого аналізу. При цьому Z-score може виступати фільтром для відсіювання некритичних коливань, що зменшує навантаження на більш обчислювально складні алгоритми.

Таким чином, Z-score є обчислювальна простим, інтерпретованим та універсальним інструментом, який суттєво підвищує ефективність систем підтримки рішень у квантових комунікаційних мережах. Його використання не лише дозволяє своєчасно виявляти критичні стани, але й забезпечує більш стабільну роботу алгоритмів виявлення аномалій у складних та динамічних середовищах передавання квантової інформації.

3.4 Оцінка взаємозв'язків параметрів квантового каналу за методом Пірсона

З урахуванням виявлених змін у поведінці основних параметрів у анамальному режимі, особливо таких, як зростання рівня шуму, зміна статистичних характеристик часу прибуття фотонів та підвищення квантової бітової похибки, постає необхідність глибшого розуміння взаємозв’язків між цими змінними. Простий опис статистичних характеристик не дозволяє встановити причинно-наслідкові залежності чи виявити приховану корельовану структуру даних. Тому доцільним наступним кроком є

проведення кореляційного аналізу за коефіцієнтом Пірсона, який дозволяє кількісно оцінити силу та напрямок лінійного зв’язку між параметрами [86, 87].

Для наочного представлення результатів кореляційного аналізу використовується теплова карта, що відображає ступінь кореляції у вигляді кольорової матриці. Такий підхід забезпечує швидке виявлення критичних залежностей, і є важливим етапом у подальшому виявленні потенційних аномалій або зовнішніх впливів на канал зв’язку. Побудова теплової карти є також підготовчим етапом до подальшої кластеризації або використання методів машинного навчання для автоматичного розпізнавання режимів роботи квантової системи [88].

З метою виявлення прихованих взаємозв’язків між фізичними параметрами квантового каналу у аномальному режимі, а також для кількісного аналізу сили лінійних залежностей між ними, було проведено кореляційний аналіз за методом Пірсона. Такий підхід дозволяє формалізовано визначити ступінь взаємозв’язку між випадковими змінними, що виникають у результаті вимірювання різних фізичних характеристик (потужність лазера, рівень шуму, час прибуття фотонів тощо), та оцінити, наскільки зміна одного параметра впливає на інший.

Коефіцієнт кореляції Пірсона для двох змінних x і y обчислюється за класичною формулою [87-89]:

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \cdot \sum_{i=1}^{n}(y_i - \bar{y})^2}}, \tag{3.6}$$

де $\bar{x}$ та $\bar{y}$ - середні значення вибірок, n - кількість спостережень.

Цей коефіцієнт набуває значень у межах від -1 до +1, де значення, близькі до ±1, свідчать про сильну лінійну залежність, а значення, близькі до 0 — про її відсутність.

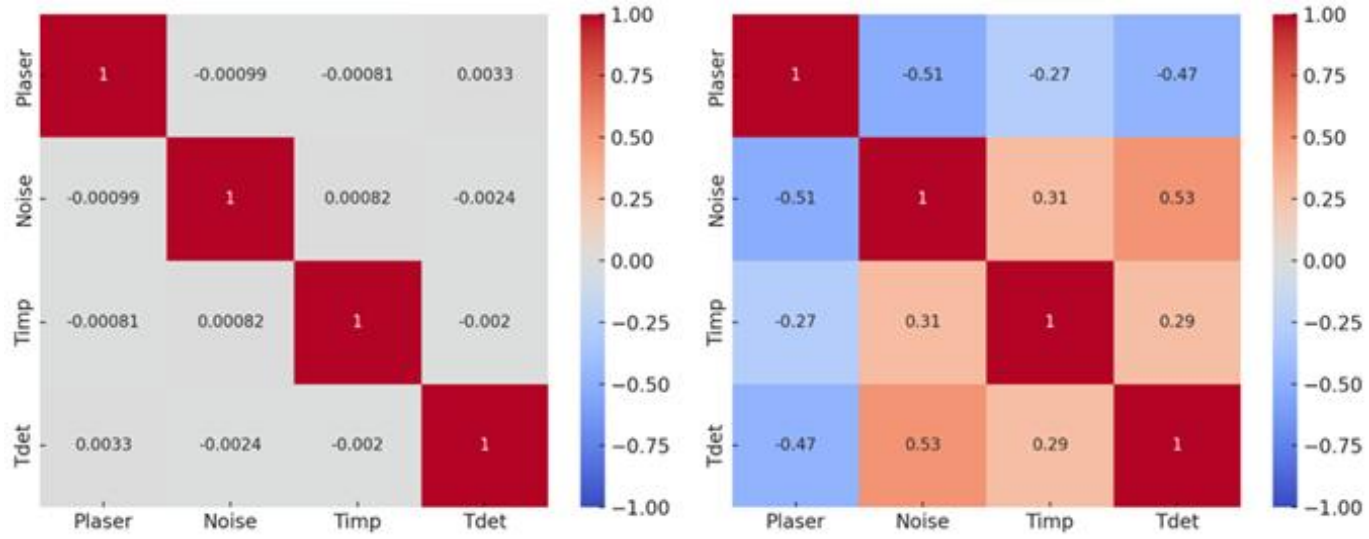
У випадку багатовимірних даних, що представлені у вигляді матриці $X \in R^{n \times p}$, де кожен стовпець відповідає окремому параметру, кореляційна структура системи описується матрицею коефіцієнтів кореляції Пірсона $R \in R^{p \times p}$, яка визначається як:

$$\mathrm{R} = \mathrm{D}^{-1} \cdot \mathrm{C} \cdot \mathrm{D}^{1}, \tag{3.7}$$

де: $\mathrm{C} = \frac{1}{n-1}(X - \bar{X})\top(X - \bar{X})$ - матриця коваріацій між параметрами; $\bar{X} \in R^{1\times p}$ - вектор середніх значень кожної змінної; D - діагональна матриця, що містить стандартні відхилення кожного параметра: $D = diag(\sigma_1, \sigma_2, \ldots, \sigma_p)$.

Застосування цього методу дозволяє сформувати повну кореляційну матрицю, в якій відображено ступінь зв'язку між усіма парами досліджуваних параметрів. Для зручності подальшого аналізу та візуального сприйняття цієї інформації результати кореляційного аналізу представлені у вигляді теплової карти (рисунок 3.1), де кожен елемент кольорової матриці відповідає значенню r_{xy}.

Така візуалізація дозволяє не лише швидко виявити ключові взаємозв'язки між параметрами, а й зафіксувати зміни у структурі залежностей під впливом переходу системи до нестаціонарного режиму.



а) б)

Рисунок 3.1 - Матриці кореляцій для двох режимів роботи квантового каналу: а) стаціонарний; б) аномальний.

У стаціонарному режимі роботи каналу зв’язку (рисунок 3.1а) спостерігається відсутність суттєвих кореляцій між усіма досліджуваними параметрами. Коефіцієнти кореляції наближаються до нуля й не перевищують значень ±0.003, що свідчить про незалежність фізичних процесів у каналі. Зокрема, потужність лазера, рівень шуму, співвідношення сигнал/шум, тривалість імпульсу та час детекції не демонструють між собою лінійного взаємозв’язку. Така структура є типовою для систем, що працюють у штатному режимі, коли усі змінні перебувають під контролем і не залежать одна від одної у межах експлуатаційної похибки.

Натомість у аномальному режимі (рисунок 3.1б) спостерігається кардинальна зміна кореляційної структури, що свідчить про порушення стабільності системи та можливу зміну режиму її функціонування. Найбільш показовим є сильний від’ємний зв’язок між потужністю лазера та рівнем шуму ($P_{laser} - Noise$, r = -0.51). Це вказує на те, що зі зменшенням потужності лазерного джерела зростає рівень фонових шумів, що може бути наслідком деградації джерела, неспівпадіння оптичних елементів або активного зовнішнього втручання.

Такі структурні зміни у матриці кореляцій свідчать про те, що у аномальному режимі спостерігається втрата незалежності параметрів, яка була притаманна системі у нормальному стані. Це, з точки зору інформаційних систем, означає появу нових інформаційних залежностей між ознаками, що раніше не взаємодіяли. У термінах системного аналізу це може бути інтерпретовано як виникнення зворотного зв’язку або перехід системи до стану з новими латентними змінними, які опосередковано впливають на її динаміку. Такі зміни критично важливі для систем безпеки, оскільки можуть бути ранніми маркерами атаки, відмови або прихованого аномального процесу в каналі зв’язку [88, 89].

Отже, результати кореляційного аналізу підтверджують припущення щодо зміни режиму роботи каналу та формують обґрунтовану основу для подальшого дослідження. Виявлені взаємозв’язки дозволяють не лише ідентифікувати найбільш підозрілі пари змінних, а й сформувати вхідний простір для алгоритмів кластерного аналізу, машинного навчання або методів виявлення аномалій. Зміна кореляційної

структури може виступати одним із ключових індикаторів для побудови систем автоматичного моніторингу стану квантового каналу зв’язку.

3.5 Аналіз розподілу параметрів за гістограмами у різних режимах роботи квантового каналу

Гістограми є важливим аналітичним інструментом, який дозволяє виявляти закономірності у розподілах даних, аналізувати варіативність параметрів і вплив атак на функціонування оптичного каналу зв’язку.

Гістограми дозволяють візуалізувати розподіли таких параметрів, як потужність імпульсу, час імпульсу, час детекції, шум та інші ключові характеристики системи. Це, своєю чергою, дає змогу оцінити відмінності між нормальними умовами роботи та умовами, що виникають під час атак. Зміни у розподілах параметрів, такі як зміщення піків, збільшення ширини або поява асиметрії, сигналізують про вплив атак на систему. Таким чином, гістограми є надійним засобом для виявлення аномалій [90-95].

Гістограма є оцінкою функції щільності ймовірності випадкової величини, що дозволяє наочно представити розподіл значень у вибірці. Її побудова відбувається у декілька етапів.

На першому етапі виконується розбиття діапазону значень випадкової величини X на певну кількість інтервалів, що називається бінінгом. Інтервали мають однакову ширину, яка визначається за формулою:

$$h = \frac{\max(X) - \min(X)}{k}, \tag{3.8}$$

де k - кількість інтервалів; $max(X)$ та $min(X)$ - максимальне та мінімальне значення випадкової величини відповідно.

Далі обчислюється частота попадання значень у кожен інтервал. Для кожного інтервалу $I_j = [a_j, b_j]$ підраховується кількість значень X, що потрапляють у цей діапазон:

$$n_j = \sum_{i=1}^{N} 1_{\mathrm{X_i \in I_j}}, \tag{3.9}$$

де $1_{X_i \in I_j}$ індикаторна функція, що дорівнює 1, якщо X_i належить інтервалу I_j, і 0 - в іншому випадку.

Наступним кроком є нормалізація частот для отримання ймовірнісного розподілу. Ймовірність потрапляння випадкової величини у конкретний інтервал обчислюється як:

$$p_j = \frac{n_j}{N}, \tag{3.10}$$

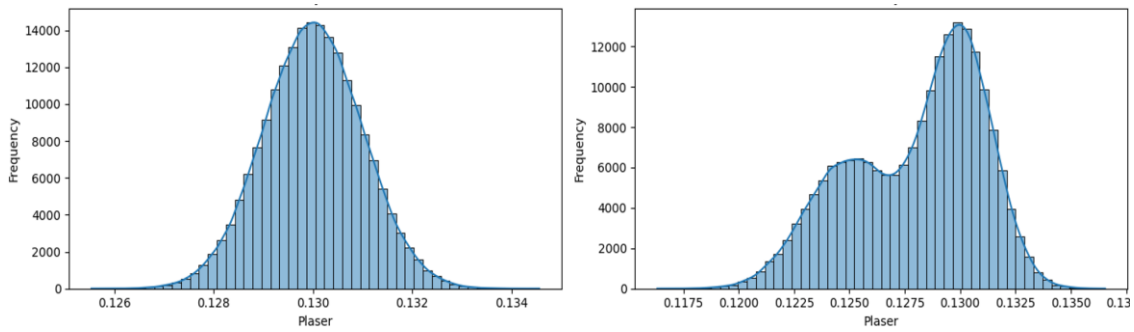
де N - загальна кількість спостережень у вибірці.

Останнім етапом є оцінка емпіричної функції щільності ймовірності. Для цього нормалізована частота ділиться на ширину інтервалу h:

$$f_j = \frac{p_j}{h}, \tag{3.11}$$

Таким чином, гістограма є графічним представленням емпіричної оцінки функції розподілу випадкової величини, що дає змогу виявляти закономірності, аномалії та особливості розподілу даних [87]. Для подальшого вивчення особливостей розподілу параметра потужності лазерного випромінювання було побудовано

гістограми частот для обох режимів функціонування каналу. Такий підхід дозволяє не лише оцінити варіативність значень, а й виявити можливі асиметрії, мультимодальність або аномальні структури, які не відображаються у зведених статистичних показниках. На рисунку 3.2 представлено гістограми розподілу значень P_{laser} у стаціонарному та аномальному режимі відповідно.



а) б)

Рисунок 3.2 – Частотний розподіл параметра інтенсивності лазерного випромінювання у різних режимах роботи квантового каналу: а) стаціонарний; б) аномальний.

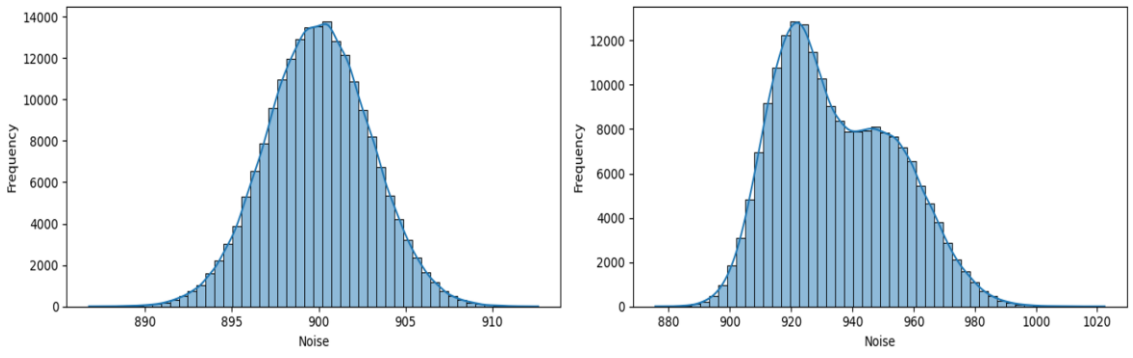
Потужність лазерного випромінювання є одним із ключових параметрів, що визначає якість генерації слабкого когерентного сигналу у квантовому каналі зв’язку. Гістограми, зображені на рисунку, відображають розподіл цього параметра у двох кардинально різних режимах роботи системи — стаціонарному та аномальному.

У стаціонарному режимі (рисунок 3.2а) гістограма має виражену симетричну одномодальну форму, яка близька до нормального розподілу. Центр розподілу припадає на значення приблизно 0.130 мкВт, що збігається із середнім значенням, визначеним під час статистичного аналізу. Висока щільність даних навколо центру та поступове спадання частот по обидва боки свідчать про високу стабільність генератора випромінювання. Відсутність значущих відхилень, «хвостів» або другорядних піків підтверджує, що система працює у контрольованих умовах без зовнішніх втручань.

Натомість у аномальному режимі (рисунок 3.2б) спостерігається суттєве спотворення форми розподілу, що проявляється у вигляді двох виражених мод. Перша - в діапазоні близько 0.125 мкВт, друга - в районі 0.130 мкВт. Такий бімодальний характер розподілу вказує на змішування двох різних режимів роботи лазера, що може бути зумовлено або періодичною зміною налаштувань, або реакцією системи на зовнішній вплив. Наявність «провалу» між модами додатково підкреслює факт розщеплення стану системи, що є ознакою нестабільності або навіть штучного втручання (наприклад, атаки на джерело світла або оптичне розгалуження сигналу).

Крім того, варто відзначити розширення діапазону значень у аномальному режимі (від ~0.117 до 0.137 мкВт), що свідчить про зростання варіативності та дисперсії. Така поведінка несумісна з нормальною роботою лазера й може негативно впливати на якість кодування та декодування квантових станів, що, у свою чергу, сприяє зростанню квантової бітової похибки.

Рівень шуму в оптичному квантовому каналі є критичним параметром, який прямо впливає на співвідношення сигнал/шум SNR, точність вимірювань і загальну достовірність переданих квантових станів. Для поглибленої оцінки поведінки цього параметра було побудовано гістограми частотного розподілу значень $Noise$ у двох режимах функціонування системи (рисунок 3.3).



а) б)

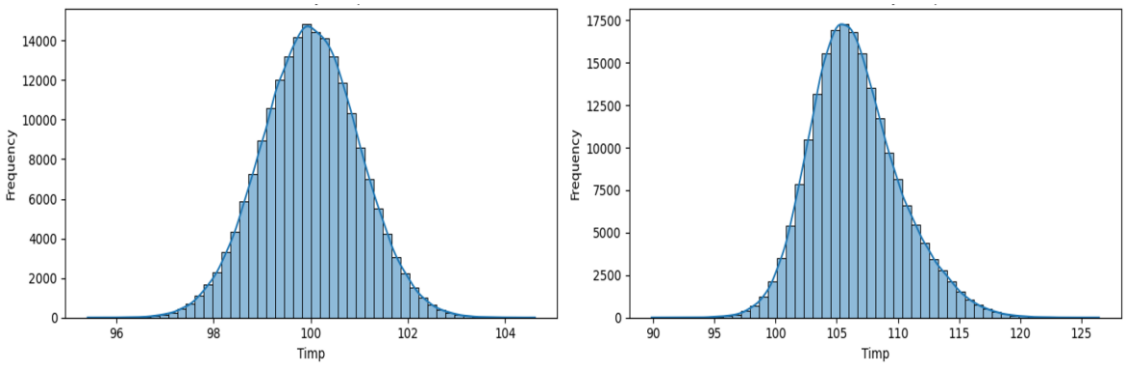
Рисунок 3.3 – Гістограма розподілу рівня шуму (Noise): а) стаціонарний режим роботи каналу зв’язку; б) аномальний режим.

У стаціонарному режимі (рисунок 3.3а) спостерігається вузький, симетричний, одномодальний розподіл, центрований навколо значення ~900 Гц. Характерна для цього режиму невелика дисперсія свідчить про відсутність істотних флуктуацій або зовнішніх збурень, які могли б впливати на електронно-оптичну систему. Така форма гістограми добре узгоджується з результатами попереднього статистичного аналізу та кореляційного дослідження, де $Noise$ не демонстрував жодних лінійних залежностей з іншими параметрами. Це підтверджує стабільність фонової складової каналу у нормальних умовах експлуатації.

У аномальному режимі (рисунок 3.3б) розподіл Noise зазнає суттєвих змін. Хоча загальна форма розподілу залишається одномодальною, спостерігається яскраво виражене зміщення центру в бік вищих значень (~925 Гц), а також розширення діапазону значень до понад 1020 Гц. Збільшення ширини розподілу є прямим свідченням підвищеної варіативності рівня шуму, що вказує на втрату контрольованості системи. Крім того, у діапазоні 940–970 Гц спостерігається локальне плато, що може свідчити про надмірну концентрацію спотворених значень - результат перешкод або високочастотних імпульсів, які супроводжують несанкціоноване втручання в канал.

Такий характер розподілу дає підстави припускати наявність нестохастичних факторів шумогенезу, які не можуть бути пояснені виключно внутрішніми флуктуаціями системи. Це може включати погіршення узгодженості оптичних компонентів або реалізацію атаки, що має на меті перевантажити приймач шумовою компонентою.

Тривалість імпульсу є важливою характеристикою сигналу в квантовому каналі зв’язку, яка визначає часову структуру переданих квантових станів і впливає на точність їхнього прийому. Відхилення від номінального значення T_{imp} може призводити до десинхронізації між передавачем і приймачем, а також до зниження ефективності детекції. Для оцінки стабільності даного параметра побудовано гістограми його розподілу у стаціонарному та аномальному режимах роботи системи (рис. 3.4).



а) б)

Рисунок 3.4 – Гістограма розподілу тривалості імпульсу: а) стаціонарний режим роботи каналу зв’язку; б) аномальний режим

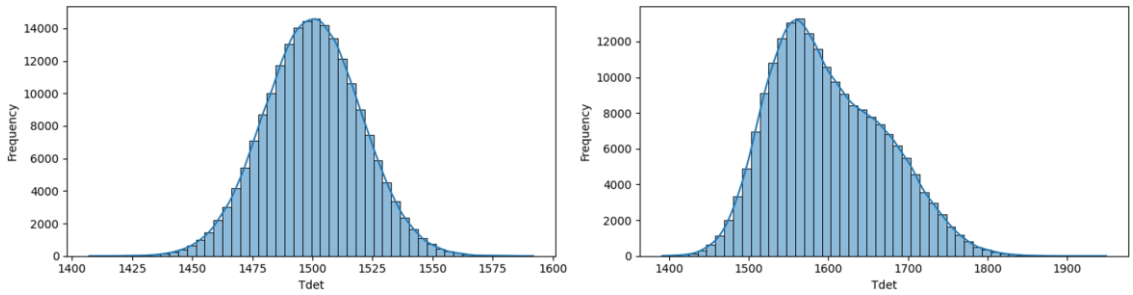
У стаціонарному режимі (рисунок 3.4а) гістограма має симетричну, вузьку, одномодальну форму, яка добре узгоджується з нормальним розподілом. Центральне значення розподілу припадає на 100 мкс, що є очікуваним і номінальним для цього типу системи. Діапазон варіацій не перевищує 5% відносно середнього, що свідчить про високу точність і повторюваність генерації імпульсів. Це підтверджує стабільну роботу таймерів і цифрових генераторів імпульсів, а також відсутність стороннього впливу на часові параметри каналу.

У аномальному режимі (рисунок 3.4б) розподіл зберігає загальну симетрію та одномодальність, однак центр гістограми зміщується до 105 мкс, а варіативність значно зростає — діапазон охоплює інтервал від 90 до 125 мкс. Такий зсув моди й розширення діапазону свідчать про появу нерегулярності у тривалості імпульсів, що може бути наслідком порушення синхронізації або розфокусування елементів генерації. Попри те, що форма розподілу не зазнає різкої деформації, зміщення середнього значення вказує на систематичний дрейф параметра, можливо зумовлений змінами навантаження, температурним впливом або інтерференційними процесами.

Особливої уваги заслуговує поява довших “хвостів” у розподілі, що характерно для аномальних або спорадичних імпульсів, які виходять за межі допустимого вікна

прийому. У контексті обробки квантових бітів це може призводити до спотворень при детекції, втрати частини ключової інформації або підвищення рівня QBER.

Час детекції є важливим параметром, який визначає момент спрацьовування приймача квантового сигналу. Відхилення цього параметра від номінальних значень може вказувати як на порушення синхронізації між передачею та прийомом, так і на затримки, спричинені фізичними або інформаційними перешкодами в каналі. На рисунку 3.5 представлено гістограми розподілу T_{detect} у стаціонарному (рис. 3.5а) та аномальному (3.5б) режимах роботи системи.



а) б)

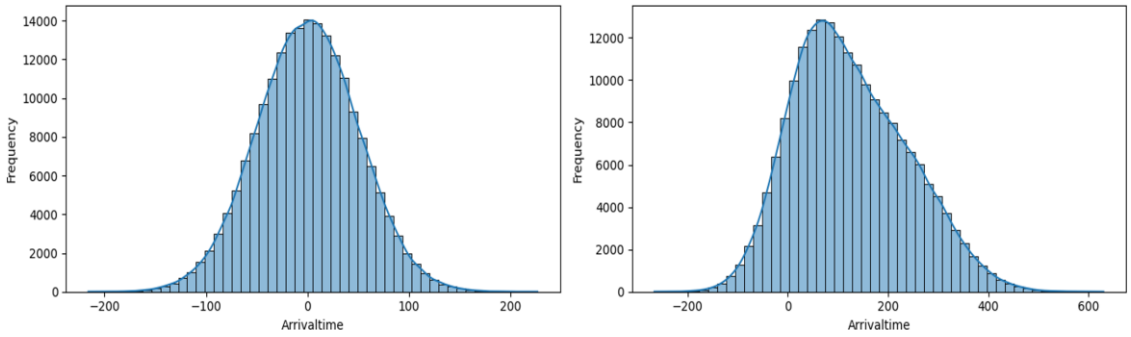
Рисунок 3.5 – Гістограма розподілу часу детекції (T_{detect}): а) стаціонарний режим роботи каналу зв’язку; б) аномальний режим

У стаціонарному режимі (рисунок 3.5а) розподіл має виразно симетричну, одномодальну форму, з піком у районі ~1500 нс. Гістограма нагадує класичний нормальний розподіл з відносно вузьким діапазоном (приблизно від 1420 до 1580 нс), що свідчить про високу повторюваність процесу детекції та відсутність критичних флуктуацій. Така форма є типовою для стабільної роботи системи, коли всі сигнали обробляються за заздалегідь визначеним часовим інтервалом. Ці результати підтверджують, що у штатному режимі фотоелектронні пристрої працюють у межах заданих технічних параметрів, не демонструючи ознак перевантаження або стороннього впливу.

У аномальному режимі (рисунок 3.5б) форма розподілу змінюється досить помітно. Хоча він залишається одномодальним, спостерігається явне зміщення моди

до вищих значень (~1560 нс), а також суттєве розширення діапазону аж до 1900 нс. Відносне збільшення частоти появи більших значень часу детекції може бути пов’язане з накладанням затримок у каналі, наприклад через збільшену довжину шляху сигналу, мультипатингові ефекти, або фазові зсуви. Наявність довгого “хвоста” праворуч від піка (від 1650 нс і вище) свідчить про рідкісні, але регулярні надмірні затримки, які можуть виникати внаслідок нештатної роботи приймального модуля.

Час прибуття фотона відображає часову точність роботи каналу зв’язку на рівні фотонної передачі. Висока стабільність цього параметра є необхідною умовою для коректної інтерпретації поляризаційних та часових характеристик кодування квантових бітів. Водночас флуктуації можуть свідчити про порушення у просторово-часовій структурі каналу або про наявність зовнішніх впливів, що викликають запізнення чи спотворення сигналів. Для дослідження цього параметра побудовано гістограми його розподілу у двох режимах функціонування (рис. 3.6).



а) б)

Рисунок 3.6 - Гістограма розподілу часу прибуття фотонів ($T_{ArrivalTime}$): а) стаціонарний режим роботи каналу зв’язку; б) аномальний режим роботи каналу

У стаціонарному режимі (рис. 3.6а) розподіл $T_{ArrivalTime}$ є симетричним, одномодальним, центрованим навколо нульової позначки, що вказує на узгодженість відліку часу відносно опорного моменту передачі. Гістограма має вигляд дзвоноподібної кривої з відносно невеликим розкидом (діапазон коливань приблизно ±220 нс), що свідчить про високу часову точність каналу та коректну синхронізацію

між передавачем і приймачем. Відсутність зміщень або асиметрії вказує на відсутність перешкод або спотворень в оптичному середовищі передачі.

У аномальному режимі (рис. 3.6б) загальна форма розподілу зберігає симетрію, однак має виразне зміщення в позитивний бік, з центром моди на рівні близько 130–150 нс, а також розширення діапазону до понад 600 нс. Спостерігається також неповна симетрія: праве “плече” гістограми більш витягнуте, що вказує на появу періодичних затримок у прибутті фотонів. Такий ефект може бути пов'язаний із:

- фазовими перешкодами (через зміщення фазових пластин або порушення кодування поляризації);

- дисперсією у волокні;

- атаками на канал з використанням квантових пам’ятей або затримуючих ліній.

Поява значного числа фотонів із відставанням у 300–600 нс може вказувати на вплив механізмів, не пов’язаних із природними флуктуаціями — наприклад, маніпуляцію шляхом динамічного зсуву часових міток, що дозволяє атакувальнику частково перехоплювати або порушувати прийом легітимним користувачем.

3.6 Кластерний аналіз експериментальних даних

У сучасних захищених системах квантової передачі інформації критично важливо оперативно аналізувати великі обсяги даних, що надходять від численних сенсорів, для своєчасного виявлення аномалій та підтримки прийняття рішень. Одним із ефективних підходів у цьому напрямку є кластеризація, яка дозволяє групувати спостереження у кластери за їх схожістю. Розглянемо математичне обґрунтування застосування алгоритмів кластеризації в контексті даної системи [95].

Нехай $x_i \in R^n$ – вектор ознак, що характеризує стан i-го спостереження, де n – кількість параметрів (наприклад, рівень шуму, бітова помилка, затримка сигналу, атенюація тощо). Загальний набір даних $\{x_1, x_2, \dots, x_m\}$ необхідно розбити на K

кластерів $C_1, C_2, \dots, C_K$. Для цього спочатку застосовують алгоритм k-середніх, який мінімізує внутрішньокластерну суму квадратів евклідових відстаней між об'єктами та їх центроїдами. Центроїд μk для кластеру C_k визначається за формулою [96]:

$$\mu_k = \frac{1}{|C_k|} \sum_{x_i \in C_k} x_i, \tag{3.12}$$

де $|C_k|$ – кількість об'єктів у кластері C_k.

Функція витрат, що підлягає мінімізації, записується як

$$J = \sum_{k=1}^{K} \sum_{x_i \in C_k} \|x_i - \mu_k\|^2, \tag{3.13}$$

де $\|\cdot\|$ позначає евклідову норму.

Алгоритм реалізується ітеративно, шляхом присвоєння кожного об'єкта найближчому центроїду та подальшим оновленням центроїдів до досягнення стабільності кластерної структури.

Оскільки точність та надійність кластеризації значною мірою залежать від правильного вибору кількості кластерів K, у даній роботі інтегровано також k-метод, який дозволяє визначити оптимальне значення K на основі аналізу внутрішньокластерної дисперсії. Метод полягає у побудові залежності функції витрат $J(K)$ від кількості кластерів. Формально ця функція має вигляд:

$$J(K) = \sum_{k=1}^{K} \sum_{x_i \in C_k} \|x_i - \mu_k\|^2, \tag{3.14}$$

За допомогою побудови графіка залежності $J(K)$ від K можна виявити «ліктьову точку» – таке значення K, при якому подальше збільшення кількості кластерів

призводить до незначного зменшення функції витрат. Вибір оптимального K таким чином дозволяє уникнути як надмірного розбиття даних на занадто багато кластерів, так і злиття неоднорідних спостережень в один кластер [96-98].

Застосування k-методу у поєднанні з алгоритмом k-середніх має кілька переваг для підтримки прийняття рішень у системі квантової передачі інформації. По-перше, воно дозволяє об'єктивно оцінити внутрішню структуру даних та адаптивно реагувати на зміни в поведінці каналу, що є критично важливим при виявленні атак або інших аномальних ситуацій. По-друге, зниження розмірності даних за допомогою методів, таких як головний компонентний аналіз (PCA), дозволяє підвищити обчислювальну ефективність алгоритмів кластеризації та забезпечити їх реальновремове застосування.

Нехай $X \in R^{m \times n}$ – матриця даних, де m – кількість спостережень, а n – кількість ознак. Матриця коваріації обчислюється за формулою:

$$C = \frac{1}{m-1} X^T X, \tag{3.15}$$

Власні вектори матриці C утворюють новий базис для простору ознак, а власні значення характеризують дисперсію даних уздовж відповідних напрямків. Застосування PCA дозволяє зберегти найбільш інформативні компоненти та зменшити розмірність простору, що покращує стабільність кластеризації.

Таким чином, інтеграція k-методу для визначення оптимальної кількості кластерів доповнює алгоритм k-середніх, забезпечуючи більш точне та адаптивне розбиття даних. Це дозволяє в режимі реального часу відстежувати зміну внутрішньої структури даних у системах квантової передачі інформації, своєчасно виявляти аномалії та автоматизувати процес підтримки прийняття рішень. Загалом, використання комплексного підходу до кластеризації, що включає як k-середніх, так і k-метод, сприяє підвищенню ефективності захищених систем та забезпеченню високого рівня кібербезпеки в умовах сучасних інформаційних технологій [99].

У процесі аналізу багатовимірних даних, отриманих під час експериментального дослідження роботи квантового каналу зв'язку, ключовим завданням є відбір інформативних комбінацій параметрів для двовимірної візуалізації результатів кластеризації. Вибір таких пар повинен ґрунтуватися не лише на статистичній варіативності даних, але й на фізичному розумінні процесів, що відбуваються у тракті «джерело–лінія–детектор». Це дозволяє двовимірним проєкціям не тільки відділяти групи точок у просторі ознак, але й виконувати діагностичну функцію - виявляти переходи між стаціонарним та нестаціонарним режимами роботи каналу, що можуть бути спричинені деградацією оптичної лінії, впливом шумів або навмисними атаками. У цьому контексті обрані пари параметрів $P_{laser} - Noise$, $P_{laser} - SNR$, $P_{laser} - T_{detect}$, $Noise - SNR$ та $T_{puls} - T_{ArrivalTime}$ - відображають ключові фізичні взаємозв'язки у функціонуванні системи, що підтверджено сучасними дослідженнями в галузі квантової криптографії та оптичних комунікацій [94].

$Plaser - Noise$. Ця пара параметрів відображає взаємозв'язок між потужністю випромінювання та рівнем шуму. Зі зростанням потужності сигналу зростає кількість зареєстрованих фотонів, проте у багатьох практичних конфігураціях одночасно збільшується і шумовий фон — як за рахунок спонтанного та стимульованого раманівського розсіювання у волокні, так і через післяімпульсність детекторів (SPAD) при високій частоті спрацьовувань. Такий зв'язок є чутливим до змін у каналі та дозволяє фіксувати переходи до нестаціонарного режиму, коли інтенсивність шумів починає корелювати з потужністю випромінювання [102].

$P_{laser} - SNR$. Співвідношення сигнал/шум прямо залежить від потужності джерела, але зростає сублінійно через обмеження, пов'язані з фоновими подіями та темновими спрацьовуваннями. Зміни SNR при фіксованому P_{laser} вказують на появу додаткових шумових процесів або деградацію чутливості приймача. Пара є фізично обґрунтованою, оскільки відображає фундаментальний баланс між корисним потоком фотонів та шумами в каналі.

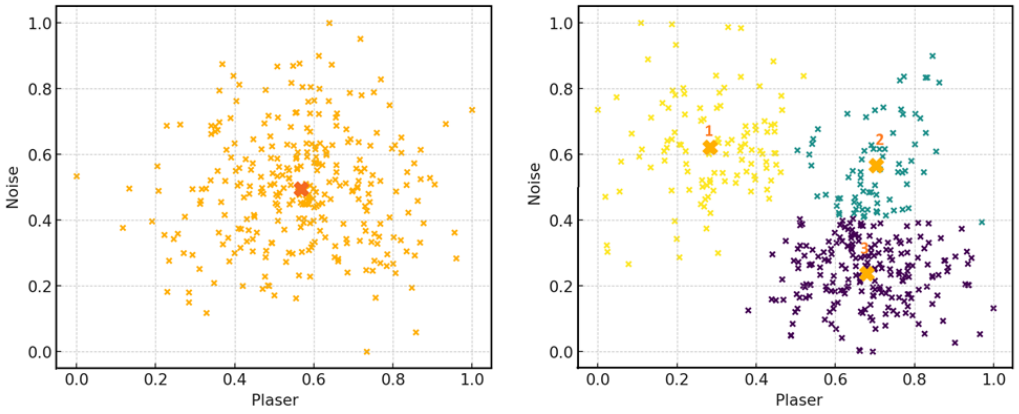
$P_{laser} - T_{detect}$. Час детектування або джиттер пов'язаний з процесом лавинного пробою у SPAD-детекторах. При більшій потужності випромінювання лавина може розвиватись швидше, зменшуючи часовий розкид, однак за високих частот рахунку можуть проявлятися ефекти «мертвого часу» та зміщення часових міток. Такий взаємозв'язок дозволяє виявляти як технічні несправності детекторів, так і спеціальні атаки типу «осліплення» [103].

$Noise - SNR$. Ця пара параметрів є інверсною відносно попередньої: збільшення шумів при фіксованому сигналі закономірно знижує SNR. Лінійна або близька до лінійної антикореляція між цими величинами є фундаментальною для фотонно-лічильних систем і може використовуватись для виявлення областей роботи з критичним співвідношенням сигнал/шум [104].

$T_{puls} - T_{ArrivalTime}$. Зв'язок між тривалістю імпульсу та часом прибуття фотона відображає вплив дисперсійних властивостей оптичного каналу. Хроматична дисперсія та температурні дрейфи у волокні призводять до уширення імпульсів і збільшення розкиду часів прибуття. Така пара є індикатором стабільності каналу та дозволяє відслідковувати деградацію або зміни у характеристиках середовища передачі [104].

Таким чином, обрані пари ознак утворюють фізично обґрунтований набір для кластерного аналізу, який відображає ключові закономірності взаємодії сигналу, шуму та часових характеристик у квантовому каналі. Використання цих пар у 2D-візуалізації дозволяє не лише розділяти дані на кластери, але й інтерпретувати причини формування кожного з них у контексті фізики процесів у системі.

На рисунку 3.7а, наведено розсіяння експериментальних точок у площині «потужність лазерного випромінювання - рівень шуму» для стаціонарного режиму роботи квантового каналу. Розподіл точок є компактним, із концентрацією біля середніх значень обох параметрів, що вказує на стабільність роботи джерела та детекторного тракту. Відсутність виражених підкластерів свідчить про сталі характеристики системи за умов мінімального впливу зовнішніх збурень [98].



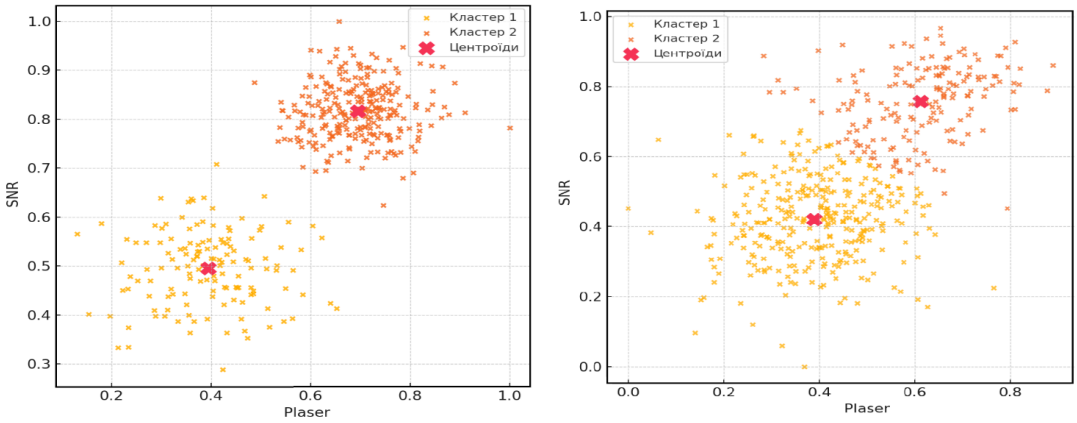
а) б)

Рисунок 3.7 - Кластеризація даних у площині «P_{laser} - $Noise$»: а) стаціонарний режим роботи каналу; б) аномальний режим роботи каналу

На рисунку 3.7б, показано результати кластеризації для нестаціонарного режиму роботи каналу, коли до вимірювань додано впливи, що імітують деградацію або атаки. Алгоритм k-means розділив вибірку на три кластери, кожен з яких відповідає відмінним станам каналу. Один з кластерів характеризується високим рівнем шуму при низькій потужності сигналу, що може бути пов’язано з індукованими шумовими процесами у волокні. Інший кластер, навпаки, відповідає високій потужності випромінювання за зниженого шуму, що відображає короткочасні стабільні інтервали роботи. Третій кластер займає проміжну область і може відповідати перехідним станам системи. Така структура розподілу підтверджує високу чутливість ознак P_{laser} та $Noise$ до змін у каналі та виправдовує їх використання для діагностики режиму роботи системи [105-107].

На рисунку 3.8а представлено результати кластеризації даних у площині «потужність лазерного випромінювання – співвідношення сигнал/шум» для стаціонарного режиму роботи квантового каналу. Спостерігається чітке розділення вибірки на два кластери, що відображає наявність двох основних станів системи: один відповідає нижчим значенням потужності сигналу та помірному SNR, інший — підвищеній потужності випромінювання та високому відношенню сигнал/шум.

Подібна структура кластерів свідчить про стабільність параметрів роботи джерела та приймача, а також про відсутність значних збурень у каналі, що могло б спричинити перехід системи у аномальний стан.



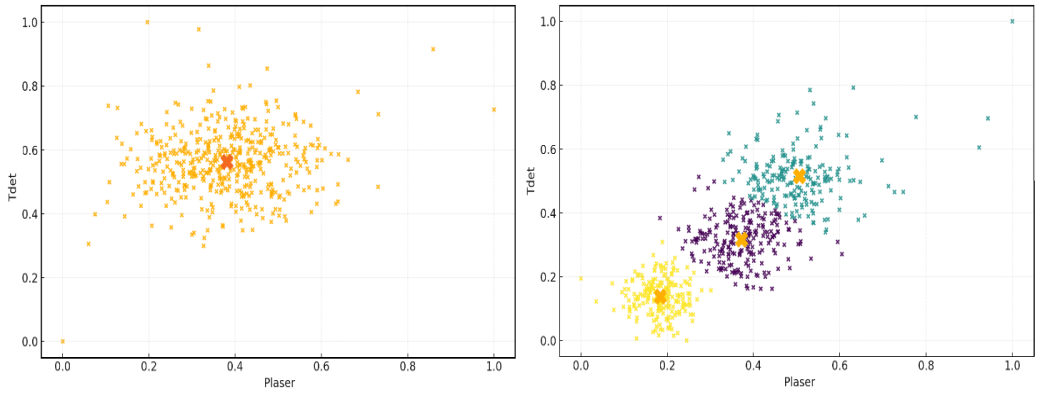
а) б)

Рисунок 3.8 - Результати кластеризації даних у площині «$P_{laser} - SNR$»: а) стаціонарний режим роботи квантового каналу; б) аномальний режим роботи квантового каналу

На рисунку 3.8б показано аналогічний розподіл для нестаціонарного режиму роботи. Хоча зберігається загальна тенденція позитивної кореляції між P_{laser} та SNR, межі кластерів стають менш чіткими, а розсіяння точок - більш вираженим. Це вказує на збільшення варіативності вимірювань та часткове перекриття станів, що характерно для режимів із флуктуаціями потужності джерела, зростанням рівня шуму або нестабільністю роботи детекторів. Такі зміни призводять до зниження контрастності між робочими станами системи та можуть бути маркером погіршення якості формування та приймання квантових бітів.

Таким чином, аналіз пари ознак «$P_{laser} - SNR$» демонструє, що ця комбінація є інформативним індикатором стабільності роботи каналу: у стаціонарних умовах спостерігається чітке групування станів, тоді як у нестаціонарних умовах кластери розмиваються, відображаючи зростання нестабільності системи.

На рисунку 3.9а показано розподіл даних у координатах «потужність лазерного випромінювання та час детектування» для стаціонарного режиму роботи квантового каналу. Розсіяння точок зосереджене в одній компактній області з незначними флуктуаціями, що вказує на стабільність як джерела випромінювання, так і процесу детектування фотонів. Часові характеристики системи залишаються узгодженими, а розподіл не демонструє ознак суттєвих відхилень, характерних для впливу зовнішніх факторів чи деградації обладнання.



а) б)

Рисунок 3.9 - Кластеризація даних у площині «$P_{laser} - T_{detect}$»:
а) стаціонарний режим роботи джерела та детекторів; б) аномальний режим

На рисунку 3.9б наведено розподіл для нестаціонарного режиму, де спостерігається розділення вибірки на три кластери з помітним розширенням діапазону значень T_{detect}. Подібна структура може свідчити про наявність декількох робочих станів системи:

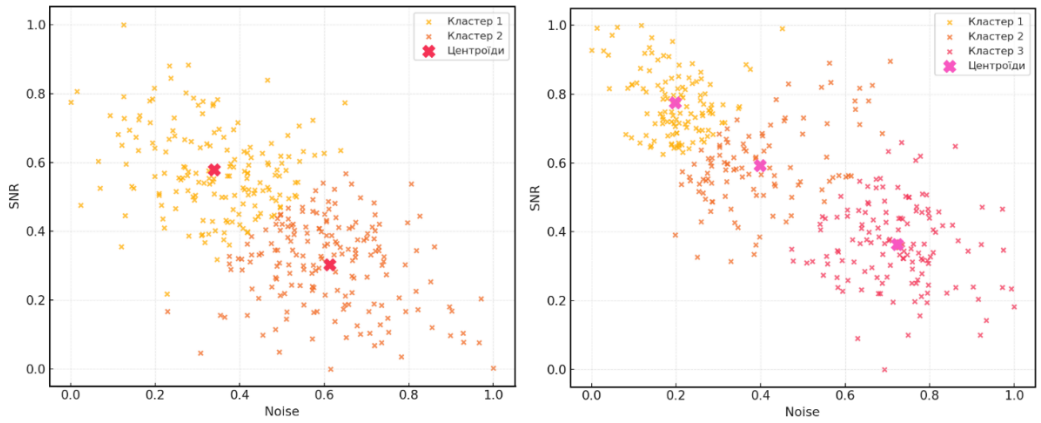
- області з низьким T_{detect} та низьким P_{laser}, що вказує на нестабільну роботу джерела;

- зони з проміжними значеннями параметрів, які можуть відображати перехідні стани;

- зони з високим T_{detect} і підвищеним P_{laser}, що можуть бути пов'язані з впливом шумових імпульсів або змінами в схемі детекторів.

Зміна структури розподілу та поява додаткових кластерів є індикаторами нестабільності каналу, які можуть призводити до збільшення похибок при відновленні квантових бітів.

На рисунку 3.10а представлено результати кластеризації даних у площині «рівень шуму - співвідношення сигнал/шум» для стаціонарного режиму роботи квантового каналу. Спостерігається характерна негативна кореляція між цими параметрами: зі зростанням шуму SNR закономірно зменшується. Алгоритм кластеризації k-means виділив дві групи точок, що відповідають різним стабільним робочим станам системи - з нижчим рівнем шуму та вищим SNR, і навпаки. Чітке розділення між кластерами вказує на стабільність параметрів і передбачувану реакцію системи на зміни шумового фону.



а) б)

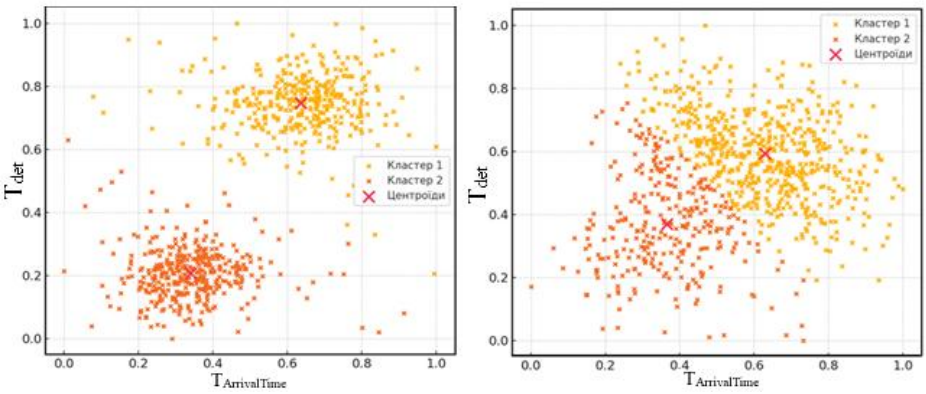
Рисунок 3.10 - Кластеризація даних у площині «$Noise - SNR$»:
а) стаціонарний режим роботи каналу передачі; б) аномальний режим роботи каналу передачі

На рисунку 3.10б зображено розподіл для нестаціонарного режиму. Тут алгоритм виявив уже три кластери, а розсіяння точок стало більш вираженим. З'являється група з високим рівнем шуму та низьким SNR, що може свідчити про

погіршення фільтрації сигналу або зростання інтенсивності фонових фотонів. Зміна структури кластерів і поява додаткової групи є індикатором нестабільності каналу, яка може призвести до підвищення ймовірності помилок при відновленні ключа.

Таким чином, пара ознак «$Noise - SNR$» є інформативним діагностичним інструментом: у стабільних умовах кластери мають чітке відокремлення, тоді як у нестабільних - їх межі розмиваються, а кількість станів системи зростає.

На рисунку 3.11а показано результати кластеризації даних у площині «час прибуття фотона ($T_{ArrivalTime}$) – ймовірність детектування (T_{detect})» для стаціонарного режиму роботи квантового каналу. Розподіл вибірки чітко поділяється на два кластери: один характеризується меншими значеннями часу прибуття та нижчою ймовірністю детектування, інший - більшим часом прибуття та підвищеним T_{detect}. Подібна структура може відображати різні стани синхронізації каналу та ефективності роботи детекторів. Чітке розділення між кластерами свідчить про стабільну роботу системи та узгодженість її часових характеристик.



а) б)

Рисунок 3.11 - Кластеризація даних у площині «$T_{ArrivalTime} - T_{detect}$»: а) стаціонарний режим роботи каналу передачі; б) аномальний режим роботи каналу передачі

На рисунку 3.11б наведено аналогічний розподіл для нестаціонарного режиму. У цьому випадку спостерігається значне розширення зон кластерів, збільшення

розсіяння точок та часткове перекриття областей. Це вказує на зростання варіативності у часі прибуття фотонів та зміни у ймовірності їх детектування. Причиною такої поведінки можуть бути флуктуації джерела, зміни у дисперсійних характеристиках оптичного каналу або нестабільність у роботі синхронізаційної системи. Погіршення розділення між кластерами є індикатором зниження часової узгодженості та стабільності прийому сигналу.

Таким чином, пара ознак «$T_{ArrivalTime} - T_{detect}$» є ефективним інструментом для моніторингу синхронізації та стабільності квантового каналу: у стабільних умовах спостерігається чітке групування даних, тоді як у нестабільних режимах розподіл стає розмитим і менш структурованим [102-112].

3.7 Методи машинного навчання

У рамках розробки інформаційної технології підтримки рішень в захищеній системі квантової передачі інформації доцільно розглянути застосування методу машинного навчання на основі багатошарового перцептрона (MLP). Такий підхід дозволяє автоматизувати процес класифікації станів квантового каналу, використовуючи набір діагностично значущих параметрів ($P_{laser}, Noise, SNR, T_{detect}, T_{ArrivalTime}$), які вже підтвердили свою ефективність під час кластеризаційного аналізу.

MLP виступатиме як інтелектуальний модуль у структурі інформаційної технології, здатний виявляти та ідентифікувати аномальні стани каналу (включно з тими, що можуть бути наслідком навмисних атак або деградації лінії) в режимі реального часу. Це дозволить підвищити точність та швидкодію процесу прийняття рішень, а також забезпечити своєчасне реагування на потенційні загрози безпеці.

Архітектура MLP передбачатиме вхідний шар, кілька прихованих шарів з нелінійними функціями активації (ReLU) та вихідний шар із softmax-активацією для

багатокласової класифікації. Навчання моделі здійснюватиметься на попередньо розмічених даних, що репрезентують різні стани каналу (стаціонарний, аномальний). Оптимізація параметрів виконуватиметься за допомогою сучасних алгоритмів (Adam, RMSprop), а для контролю якості застосовуватиметься крос-валідація.

Таким чином, інтеграція багатошарового перцептрона у захищену систему квантової передачі інформації в рамках розроблюваної інформаційної технології підтримки рішень є доцільним і перспективним напрямом. Це рішення підвищує ефективність моніторингу, стійкість системи до зовнішніх впливів і рівень кіберзахисту в умовах сучасних інформаційних загроз.

У даному дослідженні попередня розмітка даних виконувалася шляхом застосування методу кластерного аналізу k-means, що належить до категорії навчання без учителя (unsupervised learning). Використання k-means забезпечує авто-матичну класифікацію експериментальних спостережень на групи (кластери) на основі подібності статистичних характеристик, без апріорних міток. Такий підхід відповідає загальновідомій методології машинного навчання.

У контексті дослідження квантових каналів кластери інтерпретувалися як різні режими роботи системи - стаціонарний, аномальний. Кожному спостереженню було присвоєно відповідний кластер, що забезпечило отримання початкових «мітки» для подальшого аналізу.

Наступний етап передбачає застосування методу навчання з учителем, зокрема багатошарового перцептрона, який навчався на основі отриманих міток. Цей підхід дає змогу ефективно поєднати здатність кластеризації виявляти структуру даних із високою точністю класифікації, яку забезпечує навчання з учителем.

Такий гібридний підхід дозволяє розширити можливості аналізу складних фізичних даних, де початково мітки відсутні, але їх можна сформувати автоматично, а далі використати як основу для побудови надійної класифікаційної моделі, реалізованої за допомогою нейронної мережі [112-114].

Висновок до Розділу 3

У розділі продемонстровано, що поєднання класичних статистичних методів, кореляційного аналізу, візуалізації розподілів та алгоритмів кластеризації створює надійний фундамент для виявлення відхилень у квантовому каналі. Використання стандартизованих показників (Z-score) та багатовимірних ознак дозволяє своєчасно ідентифікувати критичні стани та відокремлювати їх від природних флуктуацій. Інтеграція кластеризації з багатошаровим перцептроном забезпечує автоматизовану класифікацію режимів роботи каналу й підвищує ефективність систем підтримки прийняття рішень. У результаті формується гнучка інформаційна технологія, здатна адаптивно реагувати на загрози та підвищувати надійність і безпеку квантових комунікацій.

Основні матеріали розділу викладені в публікації [53, 54, 65]

РОЗДІЛ 4. ІНТЕЛЕКТУАЛЬНІ МЕТОДИ КЛАСИФІКАЦІЇ СТАНІВ КВАНТОВОГО КАНАЛУ НА ОСНОВІ БАГАТОШАРОВОГО ПЕРЦЕПТРОНА

4.1 Підготовка даних для навчання нейронної мережі

Процес підготовки даних є ключовим етапом у створенні ефективної нейронної мережі, оскільки якість вхідних ознак безпосередньо визначає точність і узагальнювальну здатність моделі. У даному дослідженні вихідними є сирі дані квантового каналу у форматі таблиці з полями: P_{laser}; $Noise$; SNR; $T_{ArrivalTime}$; T_{detect} $Class$ (мітка, яка відображає режим роботи каналу).

Для забезпечення узгодженості процесу підготовки даних усі етапи можуть бути представлені як послідовність операцій обробки. На рисунку 4.1 наведено узагальнену схему, що відображає основні кроки від формування вікон спостереження до підготовки навчальної та тестової вибірки.

Рисунок 4.1 - Послідовність етапів формування навчальної та тестової вибірки

Формування вікон спостереження. У задачі часової класифікації, зокрема в контексті аналізу режимів роботи квантового каналу, обробка даних методом ковзного вікна (sliding window) є фундаментальним кроком, що дозволяє перекласти послідовні вимірювання в формат, придатний для навчання нейронної мережі.

Нехай маємо часову послідовність $\{x_t\}_{t=1}^{T}$, де кожен $x_t \in R^d$- багатовимірний вектор, що містить наступні параметри:

$$x_t = [\mathrm{P_{laser}}, \mathrm{Noise}, \mathrm{SNR}, \mathrm{T_{ArrivalTime}}, \mathrm{T_{detect}}], \tag{4.1}$$

Мета даного формату навчальних прикладів, $\{(X^{(i)}, y^{(i)})\}_{i=1}^{N}$, де кожний $X^{(i)}$- вектор статистичних характеристик по вікну, а $y^{(i)}$ - мітка класу цього вікна.

У даному дослідженні ширина ковзного вікна W зафіксована і дорівнює 100, а зсув (stride) позначимо як s. Початкова позиція вікна визначається як:

$$t = (i + 1)s + 1, \tag{4.2}$$

де i - індекс вікна.

Тоді i-те вікно містить послідовність точок:

$$X^{(i)} = [x_t, x_{t+1}, \dots, x_{t+W-1}], \tag{4.5}$$

Тоді $t = 1, 1 + s, 1 + 2s, \dots$ Для кожного сформованого вікна обчислюється набір статистичних характеристик (середнє значення, стандартне відхилення, мінімум, максимум, коефіцієнт варіації) окремо по кожному виміру.

Обчислення статистичних ознак. Після формування ковзних вікон спостереження наступним кроком є перетворення сирих даних у компактні та інформативні вектори ознак, що дозволяє знизити розмірність задачі й водночас зберегти ключову інформацію для навчання нейронної мережі. Для цього

використовується підхід екстракції статистичних характеристик, який є загальноприйнятим у задачах обробки часових рядів та потокових даних [6].

Кожне вікно трансформується у вектор статистичних ознак, який відображає агреговані характеристики даних у межах цього інтервалу:

$$f(i) = \left[\mu^{(i)}, \sigma^{(i)}, x_{min}^{(i)}, x_{max}^{(i)}, CV^{(i)}\right], \tag{4.6}$$

де $\mu^{(i)}$ - середнє значення; $\sigma^{(i)}$ - стандартне відхилення; $x_{min}^{(i)}$, $x_{max}^{(i)}$ - мінімальне та максимальне значення у вікні; $CV^{(i)}$- коефіцієнт варіації.

Таким чином, кожне вікно даних із «сирої» часової послідовності перетворюється на компактне подання f^i у багатовимірному просторі ознак. Сукупність таких векторів утворює матрицю:

$$F = \begin{bmatrix} f^{(1)} \\ f^{(2)} \\ \vdots \\ f^N \end{bmatrix}, \tag{4.7}$$

де N - кількість сформованих вікон.

Матриця F надалі використовується як навчальна вибірка для алгоритмів класифікації та кластеризації.

Збереження розмітки класів. У постановці задачі класифікації режимів квантового каналу розмітка класів (мітки *Class*) вже наявна на рівні окремих бітів або серій (отримана, зокрема, з попереднього кластерного аналізу). Під час переходу до ковзних вікон розміром $W = 100$ з кроком s необхідно перенести/узгодити цю розмітку на рівень вікон, не втрачаючи інформацію та не
вносячи витік даних. Формально, нехай маємо послідовність пар $\{(x_t, \ell_t)\}_{t=1}^{T}$, де $x_t \in R^d$ - вектор ознак бітового вимірювання, а $\ell_t \in \{1, \dots, K\}$ - бітова мітка класу (наприклад, *stationary, anomaly*). Для i-го вікна зі стартом $t = (i-1)s + 1$ визначимо

індексну множину $I_i = \{t, \dots, t + W - 1\}$ та оператор анотації вікна L, що відображає множину бітових міток у віконну мітку:

$$y^{(i)} = L(\{\ell_\tau : \tau \in I_i\}) \in \{1, \dots, K\}, \tag{4.8}$$

Найпростіше та на практиці стабільне правило - правило більшості:

$$y^{(i)} = arg \max_{k \in \{1,\dots,K\}} n_k^{(i)}, \qquad n_k^{(i)} = \sum_{\tau \in I_i} 1\{\ell_\tau = k\}, \tag{4.9}$$

За наявності нічий (декілька класів з однаковою кількістю бітів) впроваджується детермінований пріоритет або позначка «невизначено» з подальшою обробкою (відкидання, перерозмітка). Такий мажоритарний мепінг перетворює набір бітових міток у консистентну віконну мітку і забезпечує узгодженість між рівнями даних (біт ↔ вікно) без додаткових припущень. Ідеологічно це відповідає класу підходів агрегації слабких/шумних джерел розмітки; у загальнішому випадку, коли джерел розмітки кілька (евристики, квазі-правила, автоматичні маркери), їх корисно об’єднувати не просто голосуванням, а генеративною моделлю міток (на кшталт Snorkel), що вчиться вагам та кореляціям «джерел» і дає більш стійку агреговану розмітку.

Альтернативою жорсткій мітці є м’яка віконна анотація через пропорції класів у вікні:

$$\pi^{(i)} = \left(\frac{n_1^{(i)}}{W}, \dots, \frac{n_K^{(i)}}{W} \right) \in \Delta^{K-1}, \tag{4.10}$$

яку можна прямо використовувати як цільовий розподіл у крос-ентропійному ризику під час навчання (soft targets). Такий підхід - частковий випадок парадигми Learning from Label Proportions (LLP), де для групи/«мішка» відома лише пропорційна

розмітка, але це все одно дає узагальнюваний класифікатор на рівні окремих екземплярів та груп (формальні гарантії через EPRM). У нашому випадку «мішком» виступає вікно [108].

З погляду інформаційних технологій, етап збереження розмітки - це транзакційна операція у конвеєрі обробки даних: для кожного сформованого вікна створюється запис у таблиці WindowSet, що містить:

- ідентифікатор вікна/кадру;
- часові межі;
- вектор ознак;
- віконну мітку або розподіл;
- службові поля для аудиту.

Ця операція гарантує трасованість: завжди можна відтворити $y^{(i)}$ з первинних бітових міток $\{\ell\tau\}$.

Критично важливою є ізоляція навчання від витоків інформації. Всі вікна, що походять із одного й того самого $frame_{id}$ (або фізичного відрізка каналу), мають бути віднесені в один спліт (train/val/test) — інакше сусідні перекривні вікна з того самого фрейма «підкажуть» моделі майбутні патерни, що штучно завищить метрики [109-111].

За наявності класового дисбалансу (наприклад, «аномалія» трапляється рідше), при навчанні корисно застосовувати клас-ваги або class-balanced loss із «ефективною кількістю зразків»:

$$\alpha_y = \frac{1-\beta}{1-\beta^{n_y}}, \quad \beta \in [0,1], \tag{4.11}$$

де n_y - кількість вікон класу y.

Це дає більш стабільні оцінки для міноритарних класів без агресивного оверсемплінгу.

Нарешті, коли «бітові» мітки ℓ_t отримано з безвчительних процедур (кластеризація), їх природа може бути шумною. У таких випадках замість прямого majority vote доцільно: моделювати надійність джерел розмітки та їхню корельованість (Snorkel, data programming); залишати пропорційні цілі $\pi^{(i)}$ і оптимізувати мережу по відношенню до цих розподілів (LLP). Обидві стратегії формально обґрунтовані й добре вписуються в конвеєр інформаційної системи: модуль анотації → модуль агрегації → модуль навчання [112].

Нормалізація ознак. Підготовки даних до нормалізація виконує роль уніфікації масштабу числових ознак перед навчанням багатошарової нейронної мережі. Оскільки вихідні параметри каналу мають різну розмірність та діапазони (наприклад, потужність лазера, рівень шуму, час прибуття імпульсу), пряме подання цих величин у модель призводить до домінування ознак у метриках відстані та до погіршення умов для градієнтної оптимізації. Стандартизування або масштабування ознак зменшує цю диспропорцію, робить поверхню втрат більш «круглою» та прискорює збіжність градієнтних методів. Класичні рекомендації щодо підготовки даних для багатошарових мереж наголошують, що вирівнювання масштабу значень суттєво полегшує Backpropagation і зменшує ризик насичення нелінійностей у прихованих шарах.

У роботі застосовується післявіконне масштабування: спершу формуються ковзні вікна довжини $W = 100$ і з них обчислюються статистичні ознаки (середнє, стандартне відхилення, мінімум, максимум, коефіцієнт варіації) для кожного з обраних каналів. Лише тоді до матриці цих віконних ознак $F \in R^{N \times p}$ - кількість вікон, p - кількість ознак) застосовується нормалізація. Такий порядок (спершу агрегація, потім масштабування) відповідає інженерній практиці: ми масштабуємо саме ті «узагальнені» величини, які безпосередньо споживає модель, зберігаючи при цьому зв’язність між рівнями «біт → вікно». Обґрунтовано вибрано лінійне масштабування Min-Max на відрізок [0,1]:

$$z_{ij} = \frac{x_{ij} - m_j^{min}}{m_j^{max} - m_j^{min}}, \qquad m_j^{min} = \min_i \mathrm{x_{ij}}, m_j^{max} = \max_i \mathrm{x_{ij}}, \tag{4.12}$$

де x_{ij} - значення j - тої ознаки у i-му вікні, а z_{ij} - нормалізоване значення. Лінійне відображення до [0,1] є стандартним у статистичному аналізі й обробці часових рядів; воно легко узагальнюється на довільний інтервал $[a, b]$, що корисно у виробничих ПЗК-конвеєрах. Емпіричні дослідження показують, що вибір техніки масштабування помітно впливає на якість подальшої класифікації [13, 14].

Важливою вимогою є відсутність витоків даних у процесі масштабування. Оцінки m_j^{min}, m_j^{max} (або будь-які інші параметри нормалізації) мають обчислюватися лише на тренувальній підвибірці й заморожуватися для валідації та тесту [15].

Формування навчальної та тестової вибірок. Нехай маємо множину вікон спостереження:

$$D = \{(f_i, y_i) g_i\}_{i=1}^{N}, \tag{4.13}$$

де $f_i \in R^p$ - вектор статистичних ознак, обчислений над ковзним вікном довжини W=100; $y_i \in Y = \{1, \dots, K\}$ - клас режиму каналу; g_i - ідентифікатор «групи» (frame_id), спільний для всіх перекривних вікон, що походять з одного й того самого фрейма. Метою є побудова оцінки ризику узагальнення

$$R(h) = E_{(f,y)\sim P}\big[\ell\big(y, h(f)\big)\big], \tag{4.14}$$

де h - класифікатор, ℓ - функція втрат, а P - (невідомий) розподіл даних. Оскільки P недоступний, оцінювання виконують на відкладеній вибірці, що моделює «нові» дані.

Стандартна hold-out-оцінка ризику тестом:

$$\hat{R}_{test}(h) = \frac{1}{|\mathrm{D}_{test}|} \sum_{(f, y \in D_{test})} \ell\,(y, h(f)), \qquad (4.15)$$

є асимптотично незміщеною за умови розділення даних на статистично незалежні тренувальні та тестові підмножини. Ключове - сконструювати це розділення так, щоб уникнути витоків інформації (data leakage). Використання спільних фреймів по різних сплітах створює залежні (майже дубльовані) приклади через перекриття вікон, що веде до необґрунтовано оптимістичних метрик; уникати цього слід жорстким груповим розділенням: усі вікна з однаковим g_i належать лише одному зі сплітів.

У роботі приймаємо конфігурацію $D = D_{train} \cup D_{val} \cup D_{test}$ із частками 70%, 15%, 15%, 70% на рівні груп g (тобто спочатку випадково пермутуємо унікальні $frame_{id}$, потім відтинаємо підмножини на тренування/валідацію/тест). Така схема забезпечує незалежність тесту й валідності від тренування, дозволяє налаштовувати гіперпараметри та виконувати ранню зупинку за метриками валідації без «підглядання» в тест. Після відбору моделі тестова оцінка R^{test} використовується лише одноразово, як фінальна. Перевикористання тесту на етапі підбору гіперпараметрів спричиняє завищення якості, це явище формально продемонстровано як зміщення оцінок при спільному відборі моделі й оцінюванні.

Розподіл класів у реальних даних часто є нерівномірним, а віконна агрегація може додатково підсилювати дисбаланс. Щоб уникнути зсуву апріорних імовірностей, доцільно застосовувати стратифікацію за класом під час вибору груп у спліти: якщо позначити $p_k = P(y = k)$, то на кожному спліті бажано підтримувати $\hat{p}_k \approx p_k$

У випадках суттєвого дисбалансу рекомендовано поєднувати стратифікацію з ваговими втратами або методами class-balanced loss при навчанні. Узагальнений огляд впливу дисбалансу та інженерних контрзаходів наведено в оглядовій статті IEEE TKDE.

Коли порядок спостережень не можна вважати незалежною вибіркою (типово для часових або просторових процесів), проста IID-стратифікація є некоректною. Для

таких випадків у літературі описано блоковане/групове перехресне оцінювання: дані розбивають на часові або просторові блоки, які не перетинаються між тренуванням і валідацією/тестом; це зменшує оптимізм оцінок і краще імітує предикцію на «майбутніх» або «віддалених» регіонах. Наше розділення за $frame_{id}$ є приватним випадком блокованої валідації (group/block CV), рекомендованої для структурованих даних.

Якщо обсяг даних обмежений, для стабільнішого вибору гіперпараметрів можна застосувати перехресну валідацію на тренувальній підмножині:

$$\hat{R}_{CV} = \frac{1}{K}\sum_{k=1}^{K}\frac{1}{\left|D_{val}^{(k)}\right|}\sum_{(f,y)\in D_{val}^{(k)}} \ell\left(y, h^{(k)}(f)\right), \tag{4.16}$$

де кожна складка будується групово (за g) і, за можливості, стратифіковано за класом.

З погляду інженерії інформаційних систем, формування вибірок реалізується як крок ETL-конвеєра:

- на рівні груп g генерується випадкова перестановка;

- формується розбиття на train/val/test із фіксованим seed для відтворюваності;

- таблиці Windows та Splits з'єднуються по $frame_{id}$ для маркування кожного вікна належним сплітом;

-параметри нормалізації (мін/макс або μ, σ) обчислюються лише на Dtrain\mathcal D_{train} і зберігаються як артефакт «fit-transform», що застосовується до валідації та тесту без переобчислення.

Обрана стратегія – групово-стратифікований hold-out (70/15/15) + валідаційний моніторинг – забезпечує:

- статистичну незалежність тесту;

- коректну передачу класових часток;

- відтворюваність та трасованість у конвеєрі;

- сумісність із блокованими варіантами перехресної валідації для структурованих послідовностей.

4.2 Архітектура та навчання нейронної мережі

Проектування нейронної мережі є критично важливим етапом у створенні інформаційної технології для підтримки рішень у захищеній системі квантової передачі інформації. Архітектура моделі визначає здатність алгоритму відтворювати складні залежності між параметрами квантового каналу та відокремлювати нормальні режими функціонування від аномальних, викликаних впливами або атаками.

Вхідний опис стану будується як вектор $z \in R^L$, що утворюється векторизацією матриці $5 \times L$ (п'ять сенсорів: P_{laser}, Noise, SNR, $T_{ArrivalTime}$, T_{detect}; кількість значень у серії).

Вибір саме MLP обумовлений природою даних: часову структуру вже «згорнуто» в статистичні дескриптори, тому завданням є навчити нелінійне перетворення у табличному просторі ознак, яке «зшиває» міжсенсорні взаємодії. Теоретично клас MLP є достатньо виразним для таких відображень: існує класична теорема універсальної апроксимації, згідно з якою багатошарова мережа з неперервною ненасичувальною нелінійністю здатна апроксимувати будь-яке неперервне відображення на компактній множині з довільною точністю (тут і далі - за фіксованого числа параметрів і достатньої глибини/ширини). Це безпосередньо підтримує вибір MLP у ролі $f\theta: R^{25} \to \Delta^2$, де Δ^2 - (2-вимірний) симплекс ймовірностей для трьох класів (stationary, anomaly).

Формально мережа описується каскадом афінних перетворень та поелементних нелінійностей. Так як $n_0 = 25$ - розмірність входу, обрано три приховані шари з ширинами $n_1 = 64, n_2 = 32, n_3 = 8$ і вихід $n_4 = 3$.

У всіх прихованих шарах застосовується активаційна функція Rectified Linear Unit (ReLU). Активаційна функція визначається як:

$$\varphi(x) = \max(0, x), \qquad \acute{\varphi}(x) = \begin{cases} 1, x > 0, \\ 0, x \leq 0, \end{cases}$$

тобто на додатній півосі градієнт не згасає, а на від'ємній - занулюється. На відміну від сигмоїди чи tanh, що мають зони насичення з $| \varphi'(x) | \approx 0$, ReLU суттєво зменшує проблему «зникання градієнта», пришвидшуючи збіжність та спрощуючи оптимізацію у глибині мережі. Додаткова практична перевага - розріджені активації (частина нейронів неактивні для $x \leq 0$), що діє як м'яка регуляризація й покращує узагальнення на табличних ознаках. Ці властивості докладно розглянуті у класичних джерелах з глибинного навчання та в роботі, де ReLU було запропоновано й емпірично обґрунтовано на задачах розпізнавання.

Для стабільного масштабу сигналів на старті навчання ваги ініціалізуються за He/Kaiming-схемою, спеціально виведеною для ReLU-подібних нелінійностей. Нехай n_{in} — кількість вхідних зв'язків нейрона (fan-in). Тоді елементи матриці ваг шару беруться зі з нульовим середнім і дисперсією:

$$W_{ij} \sim N\left(0, \frac{2}{n_{in}}\right) \leftrightarrow Var[W] = \frac{2}{in}, \tag{4.17}$$

що зберігає дисперсію активацій крізь шари в початковому стані моделі й запобігає вибуху або згасанню сигналу. У поєднанні з ReLU така ініціалізація забезпечує стабільний потік градієнтів і зменшує час до збіжності.

Разом пара «ReLU + He-ініціалізація» утворює архітектурний базис для щільних шарів: ReLU надає ненасичувану нелінійність з простою похідною, а He-варіанс вирівнює масштаб активацій на старті. Цей вибір є стандартом де-факто для MLP у задачах класифікації з агрегованими ознаками й безпосередньо підвищує

надійність і швидкість навчання порівняно з сигмоїдними/гіперболічними активаціями та невідповідними схемами ініціалізації.

Вихідний шар реалізує афінне відображення $a = W_4 h_3 + b_4$ та нормалізацію softmax.

$$p_k = \frac{\exp(a_k)}{\sum_{j=1}^{3} \exp(a_j)}, \qquad k = 1,2$$

що інтерпретується як ймовірності класів і математично відображає $\mathbb{R}^2$ у Δ^2. Таке ймовірнісне кодування узгоджується з класичною постановкою багатокласової класифікації та дозволяє надалі використовувати стандартні ризики типу крос-ентропії.

Щоб зменшити коадаптацію детекторів ознак і покращити узагальнення, після кожного прихованого шару застосовується dropout з імовірністю занулення $p \approx 0.1$. На тренуванні це відповідає стохастичній масці $m_l \sim Bernoulli(1-p)$.

Ємність моделі й обчислювальна вартість у вибраній топології залишаються контрольованими. Загальна кількість параметрів дорівнює:

$$\sum_{l=1}^{4} (n_{l-1} n_l + n_l) = (25 \cdot 64 + 64) + (64 \cdot 32 + 32) + (32 \cdot 8 + 8) + (8 \cdot 3 + 3) = 4035$$

Кількість множень на один прохід – близько $\sum_{l=1}^{4} n_{l-1} n_l = 3928$, що напрактиці відповідає мілісекундній латентності інтерфейсу на звичайному CPU/GPU. У ReLU та He-ініціалізацією це забезпечує стабільну і швидку оптимізацію стохастичним градієнтним методом і його сучасними модифікаціями, що відображено у канонічних джерелах [113,114].

4.3 Оцінка та інтерпретація результатів

Метою цього підрозділу є формалізувати, як саме перевіряється коректність роботи запропонованої моделі та як інтерпретувати її вихідні ймовірності в контексті задачі багатокласової класифікації станів каналу (*stationary*, *anomaly*). Оцінювання виконується на відкладеній вибірці вікон $W = 100$, сформованій без витоку даних із навчальної частини; далі наводяться метричні визначення, критерії порівняння моделей і підходи до інтерпретації, що відповідають стандартам статистичного навчання та інженерії інформаційних систем.

Ймовірнісний вихід і правило прийняття рішення. Нехай модель на векторі ознак $z \in \mathbb{R}^d$ повертає

$$\hat{p} = (\hat{p}_1, \hat{p}_2, \hat{p}_3) = softmax\left(a^{(out)}\right) \in \Delta^2, \tag{4.18}$$

де $\hat{p}_k = P_r(\text{клас} = k|z), \sum_k \hat{p}_k = 1$.

Стандартне байсівське правило мінімізації 0–1 втрат зводиться до

$$\hat{y} = arg \max_{k \in \{1,2,3\}} \hat{p}_k, \tag{4.19}$$

а в разі асиметричних вартостей помилок рішення приймається за мінімумом очікуваного ризику $\hat{y} = argmin_k \sum_i C(k,j)\hat{p}_j$.

Для кожного класу c фіксована кількість істинно позитивних/негативних та хибно позитивних/негативних рішень: TP_c, TN_c, FP_c, FN_c. На їх основі визначаються:

Матриця помилок задає чотири числа для кожного класу: істинні позитиви (TP), хибні позитиви (FP), істинні негативи (TN) і хибні негативи (FN). Вона описує

поведінку алгоритму на даних, а всі подальші метрики - це різні «проєкції» цієї матриці на одновимірні шкали якості.

Accuracy - це частка всіх правильних відповідей серед усіх прикладів. Інтуїтивно: «який відсоток вікон модель класифікує правильно». Цей показник зручний, коли класи збалансовані і вартість помилок симетрична. У задачах із дисбалансом або коли для нас дорожчі промахи по anomaly, accuracy може вводити в оману: модель, що ігнорує рідкісний клас, усе ще може мати високу точність, бо правильно вгадує частий клас.

$$Accracy = \frac{\sum_c (TP_c + TN_c)}{N}, \tag{4.20}$$

Precision (для класу c) відповідає на запитання: «якщо модель сказала, що це клас c, то наскільки часто вона має рацію?» Це міра «чистоти» позитивних спрацювань. У нашій предметній області висока precision для anomaly означає мало хибних тривог (низький FP): якщо система сигналізує про аномалію, це майже напевно не фальстарт.

$$recision_c = \frac{TP_c}{TP_c + FP_c + \varepsilon}, \tag{4.21}$$

Recall (для класу c) відповідає на протилежне запитання: «із усіх справжніх прикладів класу c яку частку ми знайшли?» Це чутливість. Для anomaly високий recall означає, що ми «зловили» майже всі аномальні вікна (низький FN), навіть якщо при цьому зросла кількість хибних тривог (FP). У практиці завжди існує компроміс між precision і recall, який ми налаштовуємо порогом на softmax-ймовірності.

$$Recall_c = \frac{TP_c}{TP_c + FN_c + \varepsilon}, \tag{4.22}$$

F1 (для класу c) - гармонійне середнє між precision і recall; воно суворо карає ситуації, коли один показник високий, а інший низький. Тому F1 доречний, коли нам однаково важливі і мінімум хибних тривог, і мінімум пропусків. У багатокласовій постановці ми використовуємо macro-F1 як просте середнє F1 по класах: кожен клас має однакову вагу, навіть якщо він рідкісний. Саме macro-F1 зазвичай обирають основною метрикою в умовах дисбалансу та асиметрії вартостей помилок, бо вона не «маскується» частими класами і показує реальну здатність моделі розрізняти кожен стан каналу.

$$F1 = \frac{2Precision_c Recall_c}{Precision_c Recall_c + \varepsilon}, \tag{4.23}$$

Імовірнісна якість: каліброваність і лог-втрата. Оскільки вихід моделі є вектором імовірностей, важливо, щоб ці імовірності були каліброваними: для подій, яким модель призначає, скажімо, 0.8, емпірична частота правильності була близькою до 0.8. Це перевіряють діаграмою надійності (reliability diagram) та оцінкою Brier score:

$$Brier = \frac{1}{N}\sum_{i=1}^{N}\sum_{k=1}^{3}(\hat{p}_{ik} - y_{ik})^2, \tag{4.24}$$

де y_{ik} - one-hot-мітка.

Як тренувальну/контрольну метрику зручно також використовувати негативну лог-правдоподібність (log-loss):

$$NLL = -\frac{1}{N}\sum_{i=1}^{N}\log \hat{p}_i, y_i, \tag{4.25}$$

що є строго правильним скоринг-правилом і напряму пов’язане з байєсівським прийняттям рішень.

На рисунку 4.2 представлена крива навчання, це динаміка точності класифікації залежно від ітерацій. По осі абсцис відкладено номер ітерації, по осі ординат - точність, %. Суцільна синя крива відображає усереднену тренувальну точність, світло-синя лінія демонструє її миттєві коливання на міні-батчах. Чорні маркери, з’єднані штриховою лінією, позначають контрольні (перевірочні) заміри на етапах/чекпойнтах, остання точка позначена як *Final*. Сірим тлом виділено другу епоху навчання.

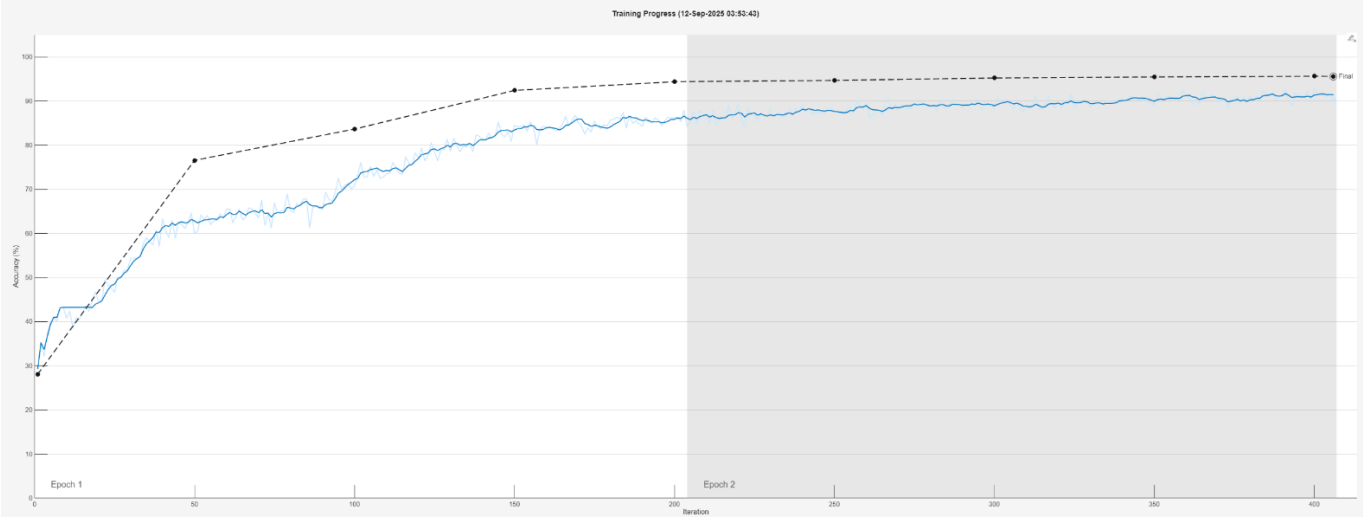


Рисунок 4.2 - Крива навчання: динаміка точності класифікації залежно від ітерацій

Упродовж першої епохи спостерігається стрімке зростання точності від приблизно 28% до понад 70%, після чого темп поліпшення поступово сповільнюється. На початку другої епохи крива входить у режим насичення: коливання зберігаються лише на рівні міні-батчів, а середня тренувальна точність стабілізується на рівні близько 90–92%. Контрольні точки демонструють досягнення

підсумкової точності порядку ≈95%, що свідчить про збіжність моделі та відсутність суттєвого розриву між тренуванням і перевіркою. Можливе невелике перевищення контрольних оцінок зумовлене відмінностями у способі обчислення (усереднення по всій вибірці проти покрокового по батчах). Загалом графік ілюструє типову еволюцію метрики під час навчання нейронної моделі з переходом від фази інтенсивного приросту до плато у другій епосі, що є індикатором досягнення стаціонарного режиму роботи класифікатора.

На рисунку 4.3 показана крива навчання: еволюція функції втрат (Loss) за ітераціями. По осі абсцис відкладено номер ітерації, по осі ординат - значення втрат. Суцільна помаранчева крива відображає усереднену тренувальну втрату, світло-помаранчева лінія показує її миттєві коливання на міні-батчах. Чорні маркери, з'єднані штриховою лінією, позначають контрольні (валідаційні) вимірювання на чекпойнтах, сірим тлом виділено другу епоху.

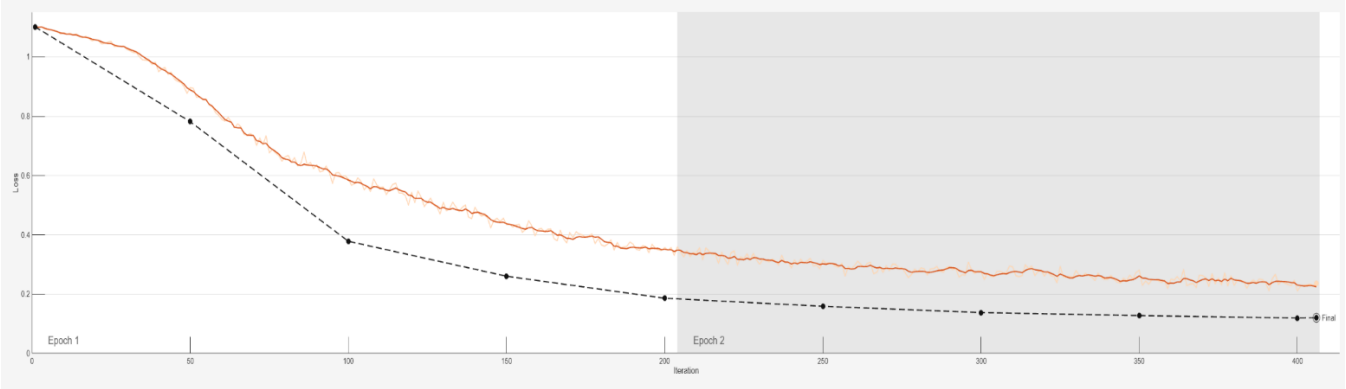


Рисунок 4.3 - Крива навчання: еволюція функції втрат (Loss) за ітераціями

Впродовж першої епохи спостерігається швидке спадання втрат від ≈1.1 до близько 0.6, надалі темп зниження уповільнюється, і на початку другої епохи крива входить у режим насичення зі стабілізацією тренувальної втрати на рівні ≈0.24–0.26 наприкінці навчання. Валідаційна втрата монотонно зменшується до ≈0.11–0.12 та лишається нижчою за тренувальну, що свідчить про коректну здатність моделі без

ознак перенавчання, залишкові флуктуації зумовлені стохастичною природою оптимізації. Таким чином, графік демонструє збіжність алгоритму та досягнення стаціонарного режиму роботи класифікатора.

На рисунку 4.4 представлена матриця плутани для докласової задачі «anomaly/stationary». По вертикалі відкладено істинні мітки, по горизонталі - передбачені моделюю.

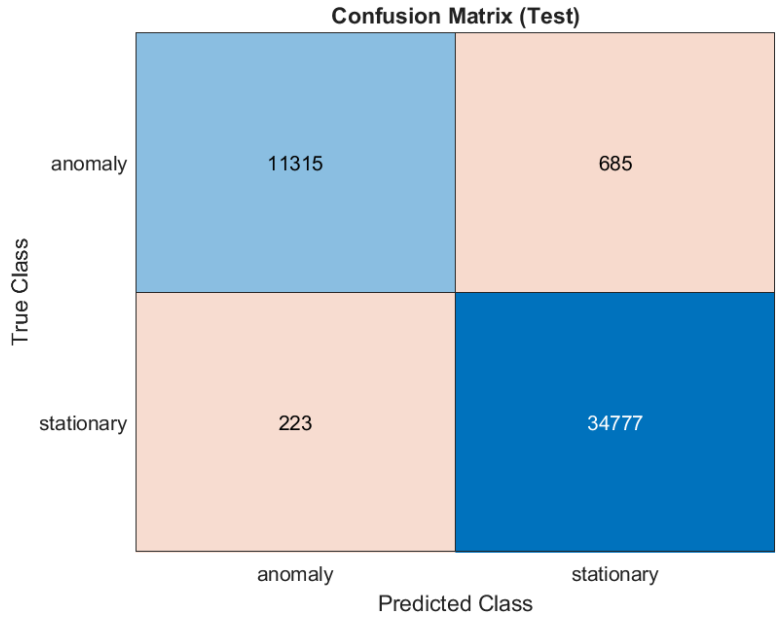


Рисунок 4.4 - Матриця плутанини (тестова вибірка) для докласової задачі «anomaly/stationary»

Підсумкову якість моделі на тесті: з 47000 прикладів коректно класифіковано 46092, що відповідає точності 98,07%. Для класу anomaly зафіксовано 11315 правильних спрацьовувань і 685 пропусків, що дає точність (precision) 98,07%, повноту (recall) 94,29% та F1-міру 96,14%; для stationary - 34777 правильних розпізнавань і 223 хибні тривоги, з точністю 98,07%, повнотою 99,36% та F1-мірою 98,71%. Усереднені показники становлять macro-F1 = 97,43% і balanced accuracy = 96,83%. Отримана структура помилок означає, що модель майже не породжує хибних тривог (FP = 223, це 0,64 % від “stationary”), але пропускає близько 5,71% аномалій

(FN = 685), тож для задач із пріоритетом виявлення аномалій доцільно зсунути поріг на користь класу anomaly або використати ваги класів.

На рис. 4.5 представлено ROC-криву моделі на тестовій вибірці (позитивний клас - anomaly).

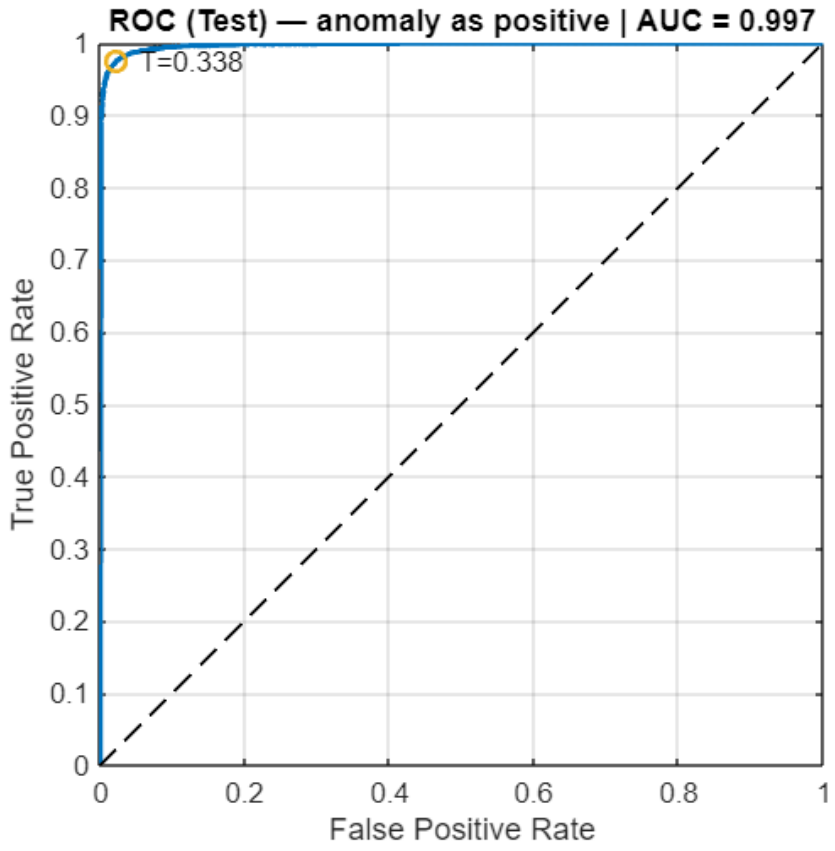


Рисунок 4.5 - ROC-крива на тестовій вибірці (позитивний клас - anomaly), AUC = 0.997

В результаті для кожного вікна багатошаровий перцептрон повертає вектор апостеріорних імовірностей $pk = [pk(anomaly), pk(stationary)]$, з якого формується дискретний вектор станів каналу $\hat{s} = (\hat{s}_1, \dots, \hat{s}_M)$, де $\hat{s} = \arg\max \mathrm{p}_k$. Подальша агрегація $\Phi(\hat{s})$ на рівні всієї серії (порог за часткою аномальних вікон або majority vote) дає фінальний домінантний стан і дозволяє локалізувати інтервали відхилень. За тестовою матрицею плутанини (див. рис. 4) модель досягає точності

98.07 %, при цьому recall для аномалій 94.29 %, а частка хибних тривог для стаціонарних станів становить лише 0.64 %. Отже, у віконному режимі класифікатор є чутливим до аномалій і водночас майже не породжує помилкових спрацьовувань, які додатково згладжуються серійним агрегатором.

4.5 Структурно-функціональна імітаційна модель управління каналом зв'язку з підсистемою моніторингу стану

На основі попередніх розділів була розроблена структурна імітаційна модель квантового каналу зв'язку, яка поєднує класичний протокол квантового розподілу ключів BB84 та вбудовану підсистеми моніторингу стану каналу, рисунок 4.6. Слід також наголосити що дана система може бути інтегрована в інші протоколи квантового розподілу ключа.

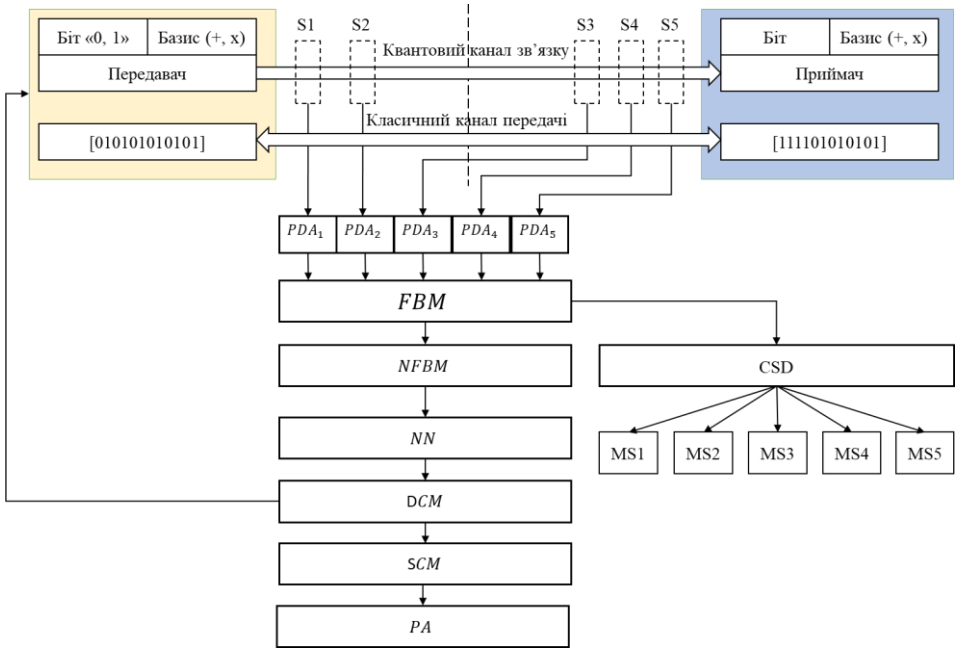


Рисунок 4.6 - Схема застосування інформаційної технологію контролю та класифікації станів в оптичних лініях передачі даних

Так як протокол BB84 було описано у попередньому розділі мова піде про реалізацію системи прийняття рішення на основі емулятора системи моніторингу каналу зв'язку.

При першому запуску система формує еталонні параметри для кожного датчика S_n. Для кожного датчика на основі початкових серій обчислюються середнє значення $\bar{x}_{si}$ та стандартне відхилення σ_{si}. Отримані значення формуються у вигляді двох векторів:

$$\bar{x}_r = \begin{bmatrix} \bar{x}_{s1}^r \\ x_{s2}^r \\ \vdots \\ \bar{x}_{s_n}^r \end{bmatrix}, \qquad \bar{\sigma}_r = \begin{bmatrix} \bar{\sigma}_{s1}^r \\ \bar{\sigma}_{s2}^r \\ \vdots \\ \bar{\sigma}_{s_n}^r \end{bmatrix}, \tag{4.26}$$

де r – початкові значення для $n-$ датчика.

Ця матриця зберігається у внутрішній пам'яті модуля CSD (модуль виявлення та локалізації критичних відхилень) та використовується як еталон.

Наступним етапом відбувається розподіл квантового ключа, кубіти відправляються по серіям.

На цьому етапі роботи системи фіксуються базові набори параметрів S1(t), S2(t), S3(t)…S5(t), що відображають інформативність вимірювальних приладів: S1, S2…S5. Вимірювальні величини задаються з урахуванням метрологічних можливостей обладнання та залишаються сталими доти, доки не відбудеться зміна конфігурації або модернізація вимірювальних засобів.

Кожен виміряний параметр надходить окремо на свій власний модуль первинного аналізу даних PDA_n. Цей модуль виконує ряд послідовних операцій:

1) Накопичення даних. Для кожного датчика S_i формується вектор-буфер фіксованої довжини L: $w_{S_i} \in \mathrm{R}^L$, який містить останні L виміряних значень сигналу.

Як тільки-но буфер заповнюється дані зберігаються у вигляді вектору та передаються наступній процедурі обробки;

2) Для датчика S_i з w_{S_i} обчислюються статистичні значення $(\bar{x}, \sigma, x_{min}, x_{max}, CV)$, та формує вектор ознак для датчика S_n (де n-номер датчику), у наступному вигляді:

$$f(S_n) = [\bar{x},\ \sigma,\ x_{min},\ x_{max},\ CV], \tag{4.27}$$

Отриманий вектор $\mathrm{f(S_n)}$ подається в модуль формування матриці ознак модулі FMB:

$$FBM = \begin{bmatrix} f(S_1) \\ f(S_2) \\ \vdots \\ f(S_n) \end{bmatrix} = \begin{bmatrix} \bar{x}_{s_1} & \sigma_{s_1} & x_{min_{s_1}} & x_{max_{s_1}} & CV_{s_1} \\ \bar{x}_{s_2} & \sigma_{s_2} & x_{min_{s_2}} & x_{max_{s_2}} & CV_{s_2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \bar{x}_{s_n} & \sigma_{s_n} & x_{min_{s_n}} & x_{max_n} & CV_{s_n} \end{bmatrix} \in R^{n\times 5} \tag{4.28}$$

Після формування матриці виконує розгалуження:

- модуль FBM передає до CSD для поточної оцінки відхилень та детекції режиму;

- передає матрицю до модуля $NFMB$ (модуль нормування матриці).

Модуль масштабує значення $NFBM$ до інтервалу [0,1] за алгоритмом min–max і подає FBM′ на вхід нейронної мережі (NN) для класифікації режиму роботи каналу.

Модуль нейронної мережі виконує бінарну класифікацію стану каналу й відносить його до одного з двох класів: стаціонарний (*stationary*) або аномальний (*anomaly*):

$$\hat{y}_i \in C = \{stationary, anomality\}, \tag{4.29}$$

Модуль DCM (модуль керування даними) отримує від нейронної мережі прогноз класу стану каналу.

На підставі цього рішення DCM подає сигнал на передавач для формування наступної серії бітів. Процедура повторюється доти, поки не буде згенеровано весь криптографічний ключ (умова зупинки).

Паралельно DCM передає кожен прогноз до модуля *SCM* (модуль акумуляції класів серій) його задача акумулювати послідовність прогнозів:

$$Y = (\hat{y}_1, \hat{y}_2, \dots \hat{y}_T), \tag{4.30}$$

де T - довжина послідовності прогнозів, дорівнює кількості відправлених серій.

В результаті формує розподіл станів каналу, передається до *SCM*.

Після завершення формування криптографічного ключа послідовність Y передається до модуля PA (агрегатор прогнозів), який визначає підсумковий клас стану каналу.

Метою модуля PA є прийняття остаточного рішення щодо домінуючого класу стану квантового каналу зв'язку на основі послідовності локальних прогнозів, сформованих попередніми модулями класифікації. Для реалізації цієї задачі застосовується метод більшості, що належить до детермінованих алгоритмів агрегування. Його ключова властивість полягає у тому, що глобальне рішення ухвалюється на основі класу, який зустрічається найчастіше у вибірці прогнозів.

Для кожного класу $c \in C$ визначимо кількість його появ:

$$n_c = \sum_{i=1}^{T} I(\hat{y}_i = Y), \tag{4.31}$$

де $I(\cdot)$ - індикаторна функція. Домінуючий клас визначається за правилом:

$$\mathrm{c}^* = arg \max_{c \in C} n_c, \tag{4.32}$$

Таким чином, глобальне рішення про стан каналу формується на основі тієї множини локальних прогнозів, яка має найбільшу частку у вибірці. Наприклад, якщо для серії довжиною $T = 200$ отримано $n_{stationary} = 118$ та $n_{anomaly} = 82$, то остаточне рішення модуля PA буде $c^* = stationary$, оскільки $118 > 82$.

Модуль CSD здійснює виявлення критичного стану на рівні окремих датчиків для поточної серії та локалізує його, визначаючи конкретний датчик або групу датчиків, на яких зафіксовано відхилення параметрів, та виконує наступні операції:

1) З матриці ознак, сформованої модулем FBM, виконується операція індексації, що полягає у виділенні першого стовпця вектора:

$$FBM^n = FBM(:1) = \begin{bmatrix} \bar{x}_{s_1}^n \\ \bar{x}_{s_2}^n \\ \vdots \\ \bar{x}_{s_i}^n \end{bmatrix}, \tag{4.34}$$

2) Розрахунок стандартизованих відхилень (Z-score) для кожного параметра:

$$|z_s| = \frac{\bar{x}_s^n - \bar{x}_s^r}{\sigma_{si}}, \tag{4.35}$$

3) Формування вектор стандартизованих відхилень:

$$Z = [Z_1, Z_2, \dots, Z_n]^T, \tag{4.36}$$

4) Вибір максимального відхилення та індексу(ів):

$$K = \{S: Z_S \max_j Z_j\} \qquad j = \in \{1, \dots, S\}, \tag{4.37}$$

Множина K містить індекси параметрів із максимальним стандартизованим відхиленням.

Аномальний стан каналу реєструється тоді, коли виконується умова: $|Z_s| > 2$, у цьому випадку фіксується перевищення порогового рівня, і відповідальний сенсор S_j (або підмножина сенсорів $\{S_j\}$) сигналізує про наявність аномалії у каналі зв'язку. Модуль CSD посилає сигнал на відповідний індикатор(и) MS_j.

Якщо $|Z_s| \geq 2$ – це стаціонарний режим роботи каналу передачі.

Всі стани фіксуються та зберігаються в пам'яті модулю CSD для подальшого аналізу.

Процес кожного разу повторюється з приходом нової серії, поки не згенерується криптографічний ключ.

Приклад реалізації модулів наведено у додатку Б, та результат виконання наведено у додатку В.

4.6 Реалізація інформаційної технології контролю та класифікації станів в оптичних лініях передачі даних

Виходячи з результатів, поданих у другому та третьому та у поточному розділі, було розроблено інформаційну технологію контролю та класифікації станів в оптичних лініях передачі даних, яка забезпечує виявлення аномалії на ранньому етапі передачі даних та визначити загального стану каналу передачі. Така реалізація дає можливість практичного застосування. Серед етапів реалізації інформаційної технології підтримки рішень слід відокремити апріорний (Етап 1) та апостеріорні етапи (Етапи 2 - Етап 7)

Інформаційної технології контролю та класифікації станів в оптичних лініях передачі даних складається з наступних етапів:

Етап 1. Апріорний етап є ключовим у реалізації інформаційної технології контролю та класифікації станів оптичних ліній. Його завдання – визначення базових характеристик, які виступають опорними для подальшого аналізу: інтенсивність

сигналу, рівень шуму, відношення сигнал/шум, час прибуття фотонів та час детектування імпульсів. Ці параметри найбільш інформативні, оскільки безпосередньо відображають фізичні процеси в оптичному середовищі та чутливі до аномалій різного походження — технічних збоїв, зовнішніх перешкод чи атак.

На цьому етапі також здійснюється навчання нейронної мережі: формуються навчальні вибірки для нормальних та аномальних режимів, дані розподіляються на тренувальну й тестову підмножини, а контроль збіжності проводиться за показниками точності та F1-score.

Особливе значення має метрологічна надійність: у разі зміни структури чи обладнання базові параметри повторно оцінюються, що гарантує коректність початкових налаштувань і достовірність подальшого аналізу;

Етап 2. На другому етапі здійснюється реєстрація характеристик оптичного каналу за допомогою вимірювальних датчиків. Фотодетектори забезпечують фіксацію моментів прибуття фотонів із високою часовою точністю, що дозволяє відстежувати синхронізацію сигналів. Вимірювачі потужності визначають інтенсивність сигналу, тоді як сенсори шуму дають змогу оцінити рівень фонових перешкод. На основі цих даних обчислюється відношення сигнал/шум, яке виступає інтегральним показником якості каналу. Часові детектори імпульсів додатково реєструють моменти їхнього спрацювання, що критично важливо для квантових протоколів. Важливою умовою є синхронна робота усіх приладів, оскільки навіть невеликі часові зсуви або похибки можуть призвести до спотворення результатів вимірювань;

Етап 3. У процесі функціонування системи всі зареєстровані параметри групуються у вектор показів, що відображає послідовність результатів вимірювань у межах заданого вікна спостереження для кожного окремого датчика. Такий підхід дає можливість не лише фіксувати поточні значення, але й аналізувати їхню динаміку у часі, що є важливим для виявлення локальних відхилень та переходів від стаціонарного режиму до аномального. Вибір довжини вікна спостереження визначає баланс між точністю оцінки стану каналу та швидкодією системи, а метод «ковзного вікна» забезпечує безперервність контролю;

Етап 4. Статистична обробка вимірюваних ознак: інтенсивність сигналу; рівень шуму; відношення сигнал/шум; час прибуття фотонів; час детектування імпульсу. Визначаються основні статистичні характеристики кожного виміряного параметра, зокрема середнє арифметичне, стандартне відхилення, мінімальне та максимальне значення, а також коефіцієнт варіації. На основі цих показників формуються вектори ознак для кожного датчика, сукупність яких утворює матрицю спостережень, що використовується як вхідні дані для подальшого аналізу;

Етап 5. Нормування елементів матриці спостережень. Здійснюється нормування елементів матриці спостережень, що дозволяє усунути масштабні відмінності між параметрами та забезпечити їхню коректну подальшу обробку. Оскільки показники мають різні діапазони значень, без нормування окремі параметри можуть штучно домінувати над іншими та викривлювати результати аналізу. Для уникнення цього значення приводяться до єдиної шкали за допомогою відповідних методів. Для цього використовується метод min-max, що зводить усі дані до інтервалу від нуля до одиниці та зберігає пропорційність між ними.

Етап 6. Класифікації режимів та локалізації відхилень. Передбачає формування рішення на основі результатів аналізу критичних станів на рівні окремих датчиків у межах поточної серії (вікна спостереження) та класифікації загального стану каналу. Прийняте рішення може стосуватися як продовження роботи системи із запуском наступної серії, так і зупинення передачі даних для з’ясування причин аномальної поведінки каналу та здійснення профілактичних заходів з метою запобігання подібним відхиленням у майбутньому;

Етап 7. Накопичення та узагальнення результатів. На цьому етапі здійснюється накопичення усіх визначених класів для кожної серії та формування узагальненого результату. На основі зібраної інформації приймається рішення щодо поточного стану каналу передачі, що дозволяє встановити його належність до стаціонарного чи аномального режиму функціонування.

На рисунку 4.7 подано схему реалізації інформаційної технології контролю та класифікації станів в оптичних лініях передачі даних, яка охоплює як апріорний етап (рис. 4.7а), так і апостеріорні етапи (рис. 4.7б).

Рисунок 4.7 - Структурна схема етапі реалізації інформаційної технології контролю та класифікації станів в оптичних лініях передачі даних: а) апріорний етап; б) апостеріорні етапи.

Запропонована послідовність етапів формує цілісну інформаційну технологію контролю та класифікації станів в оптичних лініях передачі даних. Вона поєднує апріорну підготовку з апостеріорним аналізом, забезпечуючи безперервний

моніторинг, статистичну обробку, нормування та класифікацію параметрів каналу. Завдяки використанню методів машинного навчання та врахуванню метрологічної надійності система здатна своєчасно виявляти аномалії, запобігати критичним відмовам та підтримувати стабільність і безпеку процесу передавання інформації.

Висновок до Розділу 4

Розроблений підхід доводить ефективність застосування багатошарового перцептрона (MLP) для класифікації станів квантового каналу у задачах виявлення аномалій. Використання ковзних вікон та екстракції статистичних ознак дозволяє перетворити сирі дані у компактні вектори, придатні для навчання нейронної мережі без втрати суттєвої інформації.

Архітектура MLP з оптимізованими параметрами (ReLU-активації, He-ініціалізація, Dropout-регуляризація) забезпечує високу точність класифікації й стійкість моделі до перенавчання.

За результатами тестування отримано точність 98,07 %, macro-F1 = 97,43 %, що підтверджує здатність моделі надійно відрізняти стаціонарний та аномальний режими, мінімізуючи хибні тривоги (0,64 %). Побудова ROC-кривої (AUC = 0,997) свідчить про майже ідеальну відокремлюваність класів.

Додаткове застосування процедур серійної агрегації (правило узагальненої більшості та довірчі інтервали Вілсона) дозволяє отримати остаточний домінуючий режим каналу з контрольованою похибкою.

Продемонстровані приклади з довірчими рівнями 95 % і 99 % підтверджують коректність та стабільність обраного критерію: у разі достатнього обсягу підвибірки рішення однозначне, а у випадку перетину порога інтервалом визначається потреба у збільшенні обсягу даних. Таким чином, запропонована система інтегрує машинне навчання з формальними статистичними процедурами, забезпечуючи науково

обґрунтовану, адаптивну та високоточну інформаційну технологію підтримки рішень для захищених систем квантової передачі інформації.

Основні матеріали розділу викладені в публікації [107, 115]

ВИСНОВКИ

У дисертаційній роботі розв’язано актуальне наукове завдання - створення інформаційної технології підтримки рішень в захищеній системі квантової передачі інформації, яке має істотне значення для розвитку теорії та практики безпечних телекомунікаційних систем. Комплекс проведених теоретичних і експериментальних досліджень забезпечив досягнення таких результатів:

1. Виконано аналітичний огляд сучасних методів забезпечення безпеки у квантових системах передачі інформації та підходів до підтримки прийняття рішень у сфері захищених телекомунікацій. Показано, що еволюція QKD від базових протоколів (BB84, B92) до сучасних архітектур (decoy-state, SARG04, MDI-QKD, CV-QKD, TF/PM-QKD, free-space і супутникових систем) відбувалася у відповідь на специфічні загрози й технічні обмеження, що зумовило підвищення їхньої стійкості та масштабованості. Водночас практичні реалізації залишаються вразливими до side-channel атак, що підкреслює необхідність комплексного моніторингу та інтеграції інтелектуальних інформаційних технологій.

2. Розроблено інформаційні моделі та методи статистичного аналізу й кластеризації експериментальних даних квантового каналу, які забезпечують виявлення критичних станів і відокремлення стаціонарного режиму від аномальних. Використання статистичних характеристик, кореляційного аналізу та кластеризації (k-means, PCA) дозволило формувати багатовимірний простір параметрів і забезпечити надійне розмежування режимів роботи каналу.

3. Створено математичні моделі квантового каналу, які відображають причинно-наслідкові зв’язки параметрів та враховують сценарії відмов і атак. Розроблено алгоритми виявлення аномалій на основі багатошарового перцептрона, а також методи емуляції процесів квантової передачі інформації з відтворенням штатних і критичних режимів. Реалізовано інструментальні засоби перевірки моделей із застосуванням ковзних вікон, статистичних критеріїв та процедур агрегації результатів.

4. Розроблено інформаційну технологію підтримки рішень, яка інтегрує засоби збору, обробки та інтелектуального аналізу даних у реальному часі. Система забезпечує комплексний моніторинг параметрів каналу, виявлення аномалій та їх класифікацію, а також формування стійких рішень завдяки серійній агрегації результатів. Практична апробація підтвердила її придатність для використання у реальних телекомунікаційних системах.

5. Проведено верифікацію та валідацію розроблених моделей і методів у середовищі симуляції віртуального каналу. Досягнуто високих показників ефективності: точність класифікації режимів роботи каналу становила 98,1 %, macro-F1 – 97,4 %; обчислювальна складність реалізації нейронної мережі не перевищувала 4 тис. параметрів; час реакції системи на аномальні події перебував у діапазоні 0,4–1,0 с, що відповідає вимогам роботи у реальному часі.

В результаті досліджень отримано комплексні результати, які формують науково обґрунтовану основу для побудови інтелектуальних систем підтримки рішень у квантових телекомунікаціях та забезпечують підвищення рівня їхньої безпеки і надійності.

Таким чином була досягнута мета дослідження, яка полягала в розробці та науковому обґрунтуванні інформаційної технології підтримки прийняття рішень для управління каналом передачі інформації, в умовах проявлення загроз аномалій та відмов для підвищення стійкості системи до прийнятного рівня.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Diamanti E., Lo H.-K., Qi B., Yuan Z. Practical challenges in quantum key distribution. *NPJ Quantum Information*. 2016. Vol. 2, No. 1. DOI: https://doi.org/10.1038/npjqi.2016.25.

2. Scarani V., Bechmann Pasquinucci H., Cerf N. J., Dušek M., Lütkenhaus N., Peev M. The security of practical quantum key distribution. *arXiv preprint* arXiv:0802.4155. 2009. URL: https://arxiv.org/abs/0802.4155.

3. Scarani V., Kurtsiefer C. The black paper of quantum cryptography: Real implementation problems. *arXiv preprint* arXiv:0906.4547. 2009. URL: https://arxiv.org/abs/0906.4547.

4. Zhang Q., Xu F., Chen Y.-A., Peng C.-Z., Pan J.-W. Large scale quantum key distribution: Challenges and solutions. *arXiv preprint* arXiv:1809.02291. 2018. URL: https://arxiv.org/abs/1809.02291.

5. Korchenko O., Vasiliu Y., Gnatyuk S. Modern quantum technologies of information security. *arXiv preprint*. 2010. URL: https://arxiv.org/abs/1005.5553.

6. Пінчук Д. О., Бондаренко І. О. Перспективи розвитку квантових телекомунікаційних технологій для захищеної передачі даних. Вінницький національний технічний університет, 2024. URL: https://ir.lib.vntu.edu.ua/handle/123456789/43876.

7. Sheketa V. Prospective areas of research in the development of post-quantum mechanisms of cryptanalysis of critical information. *CEUR Workshop Proceedings*. 2021. Vol. 2923. P. 31–36. URL: http://ceur-ws.org/Vol-2923/paper4.pdf.

8. Omelyanchuk A. N. Theory and experimental implementation of Josephson qubits for quantum computers. Verkin Institute for Low Temperature Physics and Engineering, NAS Ukraine, 2022. URL: https://scholar.google.com/citations?user=FhQSkMwAAAAJ.

9. Pirandola S., Andersen U. L., Banchi L., Berta M., Bunandar D., Colbeck R., Englund D., Gehring T., Lupo C., Ottaviani C., Pereira J. L., Razavi M., Shamsul Shaari J., Tomamichel M., Usenko V. C., Vallone G., Villoresi P., Wallden P. Advances in quantum

cryptography. *Advances in Optics and Photonics*. 2020. Vol. 12, No. 4. P. 1012–1236. DOI: https://doi.org/10.1364/aop.361502.

10. Hu X.-L., Cao Y., Yu Z.-W., Wang X.-B. Measurement-Device-Independent Quantum Key Distribution over asymmetric channel and unstable channel. *Scientific Reports*. 2018. Vol. 8, No. 1. DOI: https://doi.org/10.1038/s41598-018-35507-z.

11. Jain N., Gehring T., Chin H.-M., Mani H., Lupo C., Solar Nikolic D., Kordts A., Pedersen T. B., Pirandola S., Pacher C., Andersen U. L. Raw data used in Figure 3 of practical continuous-variable quantum key distribution with composable security \Dataset. Technical University of Denmark, 2022. DOI: https://doi.org/10.11583/DTU.20198891.V1.

12. Ma X., Zeng P., Zhou H. Phase-Matching Quantum Key Distribution. *Physical Review X*. 2018. Vol. 8, No. 3. DOI: https://doi.org/10.1103/physrevx.8.031043.

13. Cai W\.-Q., Li Y., Li B., Ren J.-G., Liao S.-K., Cao Y., Zhang L., Yang M., Wu J.-C., Li Y.-H., Liu W\.-Y., Yin J., Wang C.-Z., Luo W\.-B., Jin B., Lv C.-L., Li H., You L., Shu R., … Pan J.-W. Free-space quantum key distribution during daylight and at night. *Optica*. 2024. Vol. 11, No. 5. P. 647. DOI: https://doi.org/10.1364/optica.511000.

14. Ko H., Kim K.-J., Choe J.-S., Choi B.-S., Kim J.-H., Baek Y., Youn C. J. Experimental filtering effect on the daylight operation of a free-space quantum key distribution. *Scientific Reports*. 2018. Vol. 8, No. 1. DOI: https://doi.org/10.1038/s41598-018-33699-y.

15. Peev M., Pacher C., Alléaume R., Barreiro C., Bouda J., Boxleitner W., Debuisschert T., Diamanti E., Dianati M., Dynes J. F., Fasel S., Fossier S., Fürst M., Gautier J.-D., Gay O., Gisin N., Grangier P., Happe A., Hasani Y., … Zeilinger A. The SECOQC quantum key distribution network in Vienna. *New Journal of Physics*. 2009. Vol. 11, No. 7. P. 075001. DOI: https://doi.org/10.1088/1367-2630/11/7/075001.

16. Fitzke E., Bialowons L., Dolejsky T., Tippmann M., Nikiforov O., Walther T., Wissel F., Gunkel M. Scalable network for simultaneous pairwise quantum key distribution via entanglement-based time-bin coding. *PRX Quantum*. 2022. Vol. 3, No. 2. DOI: https://doi.org/10.1103/prxquantum.3.020341.

17. Yan W., Zheng X., Wen W., Lu L., Du Y., Lu Y.-Q., Zhu S., Ma X.-S. A measurement-device-independent quantum key distribution network using optical frequency comb. *NPJ Quantum Information*. 2025. Vol. 11, No. 1. DOI: https://doi.org/10.1038/s41534-025-01052-7.

18. Бондаренко І. О., Пінчук Д. О. Перспективи розвитку квантових телекомунікаційних технологій для захищеної передачі даних. Вінницький національний технічний університет, 2024. URL: https://ir.lib.vntu.edu.ua/handle/123456789/43876.

19. Bennett C. H., Brassard G. Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. Bangalore, India, 1984. P. 175–179. IEEE.

20. Lo H.-K., Ma X., Chen K. Decoy State Quantum Key Distribution. *Physical Review Letters*. 2005. Vol. 94, No. 23. DOI: https://doi.org/10.1103/physrevlett.94.230504.

21. Scarani V., Acín 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, No. 5. DOI: https://doi.org/10.1103/physrevlett.92.05790.

22. Lydersen L., Wiechers C., Wittmann C., Elser D., Skaar J., Makarov V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*. 2010. Vol. 4, No. 10. P. 686–689. DOI: https://doi.org/10.1038/nphoton.2010.214.

23. Lo H.-K., Curty M., Qi B. Measurement-Device-Independent Quantum Key Distribution. *Physical Review Letters*. 2012. Vol. 108, No. 13. DOI: https://doi.org/10.1103/physrevlett.108.130503.

24. Wang S., He D.-Y., Yin Z.-Q., Lu F.-Y., Cui C.-H., Chen W., Zhou Z., Guo G.-C., Han Z.-F. Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system. *Physical Review X*. 2019. Vol. 9, No. 2. DOI: https://doi.org/10.1103/physrevx.9.021046.

25. Wang W., Tamaki K., Curty M. Measurement-device-independent quantum key distribution with leaky sources. *Scientific Reports*. 2021. Vol. 11, No. 1. DOI: https://doi.org/10.1038/s41598-021-81003-2.

26. Grosshans F., Grangier P. Continuous variable quantum cryptography using coherent states. *Physical Review Letters*. 2002. Vol. 88, No. 5. DOI: https://doi.org/10.1103/physrevlett.88.057902.

27. Jain N., Gehring T., Chin H.-M., Mani H., Lupo C., Solar Nikolic D., Kordts A., Pedersen T. B., Pirandola S., Pacher C., Andersen U. L. Raw data used in Figure 3 of practical continuous-variable quantum key distribution with composable security \Dataset. Technical University of Denmark, 2022. DOI: https://doi.org/10.11583/DTU.20198891.V1.

28. Pirandola S., Laurenza R., Ottaviani C., Banchi L. Fundamental limits of repeaterless quantum communications. *Nature Communications*. 2017. Vol. 8. Article 15043. DOI: https://doi.org/10.1038/ncomms15043.

29. Curty M., Azuma K., Lo H.-K. Simple security proof of twin-field type quantum key distribution protocol. *NPJ Quantum Information*. 2019. Vol. 5, No. 1. DOI: https://doi.org/10.1038/s41534-019-0175-6.

30. Chen J.-P., Zhang C., Liu Y., Jiang C., Zhang W., Hu X.-L., Guan J.-Y., Yu Z.-W., Xu H., Lin J., Li M.-J., Chen H., Li H., You L., Wang Z., Wang X.-B., Zhang Q., Pan J.-W. Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km. *Physical Review Letters*. 2020. Vol. 124, No. 7. DOI: https://doi.org/10.1103/physrevlett.124.070501.

31. Liao S.-K., Cai W\.-Q., Liu W\.-Y., Zhang L., Li Y., Ren J.-G., Yin J., Shen Q., Cao Y., Li Z.-P., Li F.-Z., Chen X.-W., Sun L.-H., Jia J.-J., Wu J.-C., Jiang X.-J., Wang J.-F., Huang Y.-M., Wang Q., Pan J.-W. Satellite-to-ground quantum key distribution. *Nature*. 2017. Vol. 549, No. 7670. P. 43–47. DOI: https://doi.org/10.1038/nature23655.

32. Ko H., Kim K.-J., Choe J.-S., Choi B.-S., Kim J.-H., Baek Y., Youn C. J. Experimental filtering effect on the daylight operation of a free-space quantum key distribution. *Scientific Reports*. 2018. Vol. 8, No. 1. DOI: https://doi.org/10.1038/s41598-018-33699-y.

33. Cai W\.-Q., Li Y., Li B., Ren J.-G., Liao S.-K., … Pan J.-W. Free-space QKD during daylight and at long distances. *Optica*. 2024. Vol. 11, No. 5. P. 647–655. DOI: https://doi.org/10.1364/OPTICA.11.000647.

34. Yin J., Li Y.-H., Liao S.-K., Yang M., Cao Y., Zhang L., Ren J.-G., Cai W\.-Q., Liu W\.-Y., Li S.-L., Shu R., Huang Y.-M., Deng L., Li L., Zhang Q., Liu N.-L., Chen Y.-A., Lu C.-Y., Wang X.-B., … Pan J.-W. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature*. 2020. Vol. 582, No. 7813. P. 501–505. DOI: https://doi.org/10.1038/s41586-020-2401-y.

35. Brassard G., Lütkenhaus N., Mor T., Sanders B. C. Limitations on practical quantum cryptography. *Physical Review Letters*. 2000. Vol. 85, No. 6. P. 1330–1333. DOI: https://doi.org/10.1103/PhysRevLett.85.1330.

36. Hwang W\.-Y. Quantum key distribution with high loss: Toward global secure communication. *Physical Review Letters*. 2003. Vol. 91, No. 5. DOI: https://doi.org/10.1103/physrevlett.91.057901.

37. Rosenberg D., Harrington J. W., Rice P. R., Hiskett P. A., Peterson C. G., Hughes R. J., Lita A. E., Nam S. W., Nordholt J. E. Long-distance decoy-state quantum key distribution in optical fiber. *Physical Review Letters*. 2007. Vol. 98, No. 1. DOI: https://doi.org/10.1103/physrevlett.98.010503.

38. Qi B., Fung C.-H. F., Lo H.-K., Ma X. Time-shift attack in practical quantum cryptosystems. *Quantum Information and Computation*. 2007. Vol. 7, No. 1–2. P. 73–82. URL: https://arxiv.org/abs/quant-ph/0512080.

39. Fung C.-H. F., Qi B., Tamaki K., Lo H.-K. Phase-remapping attack in practical quantum-key-distribution systems. *Physical Review A*. 2007. Vol. 75, No. 3. DOI: https://doi.org/10.1103/PhysRevA.75.032314.

40. Gisin N., Fasel S., Kraus B., Zbinden H., Ribordy G. Trojan-horse attacks on quantum-key-distribution systems. *Physical Review A*. 2006. Vol. 73, No. 2. DOI: https://doi.org/10.1103/PhysRevA.73.022320.

41. Gisin N., Fasel S., Kraus B., Zbinden H., Ribordy G. Trojan-horse attacks on quantum-key-distribution systems. *Physical Review A*. 2006. Vol. 73, No. 2. DOI: https://doi.org/10.1103/physreva.73.022320(https://doi.org/10.1103/physreva.73.022320).

42. Fung C.-H. F., Tamaki K., Qi B., Lo H.-K., Ma X. Security proof of quantum key distribution with detection efficiency mismatch. *arXiv preprint* arXiv:0802.3788. 2008. DOI: https://doi.org/10.48550/ARXIV.0802.3788.

43. Shor P. W., Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*. 2000. Vol. 85, No. 2. P. 441–444. DOI: https://doi.org/10.1103/physrevlett.85.441.

44. Ma X., Qi B., Zhao Y., Lo H.-K. Practical decoy state for quantum key distribution. *Physical Review A*. 2005. Vol. 72, No. 1. DOI: https://doi.org/10.1103/physreva.72.012326.

45. Long N. K., Malaney R., Grant K. J. A survey of machine learning assisted continuous-variable quantum key distribution. *Information*. 2023. Vol. 14, No. 10. Article 553. DOI: https://doi.org/10.3390/info14100553.

46. Jain A. K. Data clustering: 50 years beyond K-means. *Pattern Recognition Letters*. 2010. Vol. 31, No. 8. P. 651–666. DOI: https://doi.org/10.1016/j.patrec.2009.09.011(https://doi.org/10.1016/j.patrec.2009.09.011)

47. Galvão L. Q., de Sousa D. J. G., Dias M. A., Neto N. A. F. Neural network for excess noise estimation in continuous-variable quantum key distribution under composable finite-size security (Version 1). *arXiv preprint* arXiv:2507.23117. 2025. DOI: https://doi.org/10.48550/ARXIV.2507.23117.

48. Zhang Z.-K., Liu W\.-Q., Qi J., He C., Huang P. Automatic phase compensation of a continuous-variable quantum-key-distribution system via deep learning. *Physical Review A*. 2023. Vol. 107, No. 6. DOI: https://doi.org/10.1103/physreva.107.062614

49. ID Quantique. Clavis XG QKD System. 2022. URL: https://www.idquantique.com/quantum-safe-security/products/clavis-xg-qkd-system/.

50. ID Quantique. Clavis XG QKD System. 2022. URL: https://www.idquantique.com/quantum-safe-security/products/clavis-xg-qkd-

system/(https://www.idquantique.com/quantum-safe-security/products/clavis-xg-qkd-system/).

51. Chen T.-Y., Jiang X., Tang S.-B., Zhou Z., Xiao X., Huang H., … Pan J.-W. Implementation of a 46-node quantum metropolitan area network. *arXiv preprint* arXiv:2109.04736. 2021. URL: https://arxiv.org/pdf/2109.04736.

52. European Commission. CEF2 Digital – The EuroQCI initiative (call fiche). 27 March 2025. URL: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/cef/wp-call/2024/call-fiche_cef-dig-2024-euroqci_en.pdf.

53. Lyfar V., Lyfar O., Zynchenko V. Methods of intelligent data analysis using neural networks in diagnosis. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska*. 2024. Vol. 14, No. 2. P. 109–112. DOI: https://doi.org/10.35784/iapgos.5746.

54. Зінченко В. Л., Лифар В. О. Інтелектуальний аналіз інформаційних потоків у квантових системах передачі інформації. *Problems of Control and Informatics*. 2024. Vol. 69, No. 1. P. 80–86. DOI: https://doi.org/10.34229/1028-0979-2024-1-7.

55. Martinez-Mosquera D., Navarrete R., Luján-Mora S., Recalde L., Andrade-Cabrera A. Integrating OLAP with NoSQL databases in big data environments: Systematic mapping. *Big Data and Cognitive Computing*. 2024. Vol. 8, No. 6. Article 64. DOI: https://doi.org/10.3390/bdcc8060064.

56. Georgieva-Trifonova T. Warehousing and OLAP analysis of bibliographic data. *Intelligent Information Management*. 2011. Vol. 3, No. 5. P. 190–197. DOI: https://doi.org/10.4236/iim.2011.35023.

57. Wagner T., Kampermann H., Bruß D., Kliesch M. Pauli channels can be estimated from syndrome measurements in quantum error correction. *Quantum*. 2022. Vol. 6. Article 809. DOI: https://doi.org/10.22331/q-2022-09-19-809.

58. Mastromichalakis S. ALReLU: A different approach on Leaky ReLU activation function to improve neural networks performance. *arXiv preprint* arXiv:2012.07564. 2020. DOI: https://doi.org/10.48550/arXiv.2012.07564.

59. Maniatopoulos A., Mitianoudis N. Learnable Leaky ReLU (LeLeLU): An alternative accuracy-optimized activation function. *Information*. 2021. Vol. 12, No. 12. Article 513. DOI: https://doi.org/10.3390/info12120513.

60. Datta L. A survey on activation functions and their relation with Xavier and He normal initialization. *arXiv preprint* arXiv:2004.06632. 2020. DOI: https://doi.org/10.48550/arXiv.2004.06632(https://doi.org/10.48550/arXiv.2004.06632).

61. Jagtap A. D., Kawaguchi K., Karniadakis G. E. Locally adaptive activation functions with slope recovery term for deep and physics-informed neural networks. *arXiv preprint* arXiv:1909.12228. 2019. DOI: https://doi.org/10.48550/arXiv.1909.12228.

62. Mei S., Montanari A., Nguyen P.-M. A mean field view of the landscape of two-layers neural networks. *arXiv preprint* arXiv:1804.06561. 2018. DOI: https://doi.org/10.48550/arXiv.1804.06561.

63. Koudia S., Oleynik L., Bayraktar M., Rehman J. u., Chatzinotas S. Physical layer aspects of quantum communications: A survey. *IEEE preprint*. 2024.

64. Kim J.-H., Kim Y., Im D.-G., Lee C.-H., Chae J.-W., Scarcelli G., Kim Y.-H. Noise resistant quantum communications using hyperentanglement. *Optica*. 2021. Vol. 8, No. 12. P. 1524–1530. DOI: https://doi.org/10.1364/OPTICA.442240.

65. Zinchenko V. L., Lyfar V. O. Information and mathematical model of quantum communication channel state control processes. *Environmental Safety and Natural Resources*. 2024. Vol. 51, No. 3. P. 151–160. DOI: https://doi.org/10.32347/2411-4049.2024.3.151-160.

66. Pljonkin A., Rumyantsev K., Singh P. K. Synchronization in quantum key distribution systems. *arXiv preprint*. 2018. URL: https://arxiv.org/abs/1801.06499.

67. Waks E., et al. Tools for the performance optimization of single-photon quantum key distribution. *NPJ Quantum Information*. 2020.

68. Pljonkin A., Rumyantsev K., Singh P. K. Synchronization in quantum key distribution systems. *arXiv preprint*. 2018. URL: https://arxiv.org/abs/1801.06499.

69. Calderaro L., Stanco A., Agnesi C., Avesani M., Dequal D., Villoresi P., Vallone G. Fast and simple qubit based synchronization for quantum key distribution. *Physical

Review Applied*. 2020. Vol. 13. Article 054041. DOI: https://doi.org/10.1103/PhysRevApplied.13.054041.

70. Hdaib M., Rajasegarar S., Pan L. Quantum deep learning based anomaly detection for enhanced network security. *Quantum Machine Intelligence*. 2024. Vol. 6. Article 26. DOI: https://doi.org/10.1007/s42484-024-00163-2.

71. Rajendran V. P., Perumalsamy D., Ponnusamy C., Kalaimannan E. An efficient continuous variable quantum key distribution with parameter optimization using elitist elk herd random immigrants optimizer and adaptive depthwise separable convolutional neural network. *Future Internet*. 2025. Vol. 17, No. 7. Article 307. DOI: https://doi.org/10.3390/fi17070307.

72. Asres M. W., Omlin C. W., Wang L., Yu D., Parygin P., Dittmann J., Karapostoli G., Seidel M., Venditti R., Lambrecht L., Usai E., Ahmad M., Menendez J. F., Maeshima K., the CMS HCAL Collaboration. Spatio temporal anomaly detection with graph networks for data quality monitoring of the hadron calorimeter. *Sensors*. 2023. Vol. 23, No. 24. Article 9679. DOI: https://doi.org/10.3390/s23249679.

73. Hammad A., Nojiri M. M., Yamazaki M. Quantum similarity learning for anomaly detection. *Journal of High Energy Physics*. 2025. Article 81. DOI: https://doi.org/10.1007/JHEP02(2025)081.

74. Frieden B. R. Introduction to statistical methods: Estimating the mean, median, variance, S/N, and simple probability. In: *Probability, Statistical Optics, and Data Testing* (Springer Series in Information Sciences, Vol. 10). Berlin, Heidelberg: Springer, 2001. P. 243–276. DOI: https://doi.org/10.1007/978-3-642-56699-8_9.

75. Frieden B. R. Introduction to statistical methods: Estimating the mean, median, variance, S/N, and simple probability. In: Probability, Statistical Optics, and Data Testing (Springer Series in Information Sciences, Vol. 10). Berlin, Heidelberg: Springer, 2001. P. 243–276. DOI: https://doi.org/10.1007/978-3-642-56699-8_9.

76. Scheller D. S. Central tendency. In: *Elementary Statistics for Public Administration*. Cambridge: Cambridge University Press, 2024. DOI: https://doi.org/10.1017/9781009439930.

77. Darling H. S. Do you have a standard way of interpreting the standard deviation? A narrative review. *Cancer Research, Statistics, and Treatment*. 2022. Vol. 5, No. 4. P. 728–733. DOI: https://doi.org/10.4103/crst.crst_284_22.

78. Rakrak M. Central tendency and data distribution: How to choose the right measure for accurate analysis. *International Journal of Literacy and Education*. 2025. Vol. 5, No. 1. P. 71–75. DOI: https://doi.org/10.22271/27891607.2025.v5.i1b.253.

79. Santos C., Dias C. Note on the coefficient of variation properties. *Brazilian Electronic Journal of Mathematics*. 2021. Vol. 2, No. 4. P. 101–111. DOI: https://doi.org/10.14393/BEJOM.v2.n4.2021.58062.

80. Anhøj J., Wentzel Larsen T. Sense and sensibility: On the diagnostic value of control chart rules for detection of shifts in time series data. *BMC Medical Research Methodology*. 2018. Vol. 18. Article 100. DOI: https://doi.org/10.1186/s12874-018-0564-0.

81. Thrun M. C., Gehlert T., Ultsch A. Analyzing the fine structure of distributions. *arXiv preprint* arXiv:1908.06081. 2019. DOI: https://doi.org/10.48550/arXiv.1908.06081

82. Paulauskas N., Baskys A. Application of histogram-based outlier scores to detect computer network anomalies. *Electronics*. 2019. Vol. 8, No. 11. Article 1251. DOI: https://doi.org/10.3390/electronics8111251.

83. Nassar M. Cumulative histogram as a feature selection technique for anomaly detection. *Multimedia Tools and Applications*. 2024. DOI: https://doi.org/10.1007/s11042-023-17617-7.

84. Benedetti M., Lloyd E., Sack S., Fiorentini M. Parameterized quantum circuits as machine learning models. *Quantum Science and Technology*. 2019. Vol. 4, No. 4. Article 043001. DOI: https://doi.org/10.1088/2058-9565/ab4eb5.

85. Iglewicz B., Hoaglin D. C. How to detect and handle outliers. *The ASQC Basic References in Quality Control: Statistical Techniques*. Vol. 16. Milwaukee: ASQC Quality, 1993.

86. Jiang S., Chen Y., Wang J. Hybrid quantum-classical anomaly detection for cyber-physical systems. *IEEE Transactions on Industrial Informatics*. 2023. Advance online publication. DOI: https://doi.org/10.1109/TII.2023.3261400.

87. Saccenti E., Hendriks M. H. W. B., Smilde A. K. Corruption of the Pearson correlation coefficient by measurement error and its estimation, bias, and correction under different error models. *Scientific Reports*. 2020. Vol. 10. Article 438. DOI: https://doi.org/10.1038/s41598-019-57247-4.

88. Rahadian H., Bandong S., Widyotriatmo A., Joelianto E. Image encoding selection based on Pearson correlation coefficient for time series anomaly detection. *Alexandria Engineering Journal*. 2023. Vol. 82. P. 304–322. DOI: https://doi.org/10.1016/j.aej.2023.09.070.

89. Schummer P., del Rio A., Serrano J., Jimenez D., Sánchez G., Llorente Á. Machine learning-based network anomaly detection: Design, implementation, and evaluation. *AI*. 2024. Vol. 5, No. 4. P. 2967–2983. DOI: https://doi.org/10.3390/ai5040143.

90. Kim H. Y. Statistical notes for clinical researchers: Covariance and correlation. *Korean Journal of Anesthesiology*. 2018. Vol. 71, No. 5. P. 353–358. DOI: https://doi.org/10.4097/kja.d.18.00204.

91. Malo P., Viitasaari L., Gorskikh O., Ilmonen P. Non parametric structural change detection in multivariate systems. *arXiv preprint* arXiv:1805.08512. 2018. DOI: https://doi.org/10.48550/arXiv.1805.08512.

92. Jin Y., Liu X., Hu B., Walker J., Wang K., Wu W., Zhong T. Negative feedback matters: Exploring positive and negative correlations for time series anomaly detection. *Electronics*. 2025. Vol. 14, No. 10. Article 2068. DOI: https://doi.org/10.3390/electronics14102068.

93. Paulauskas N., Baskys A. Application of histogram based outlier scores to detect computer network anomalies. *Electronics*. 2019. Vol. 8, No. 11. Article 1251. DOI: https://doi.org/10.3390/electronics8111251.

94. Nassar M., Salama R. A., Saleeb A. A., El bahnasawy N. A., Ahmed H. E. H., Abd El Samie F. E. Cumulative histogram as a feature selection technique for anomaly detection.

Multimedia Tools and Applications. 2025. Vol. 84. P. 10095–10107. DOI: https://doi.org/10.1007/s11042-023-17617-7.

95. Panić B., Klemenc J., Nagode M. Optimizing the estimation of a histogram bin width — Application to the multivariate mixture model estimation. *Mathematics*. 2020. Vol. 8, No. 7. Article 1090. DOI: https://doi.org/10.3390/math8071090.

96. Ahmed M., Seraj R., Islam S. M. S. The k-means algorithm: A comprehensive survey and performance evaluation. *Electronics*. 2020. Vol. 9, No. 8. Article 1295. DOI: https://doi.org/10.3390/electronics9081295.

97. Ahmed M., Seraj R., Islam S. M. S. The k-means algorithm: A comprehensive survey and performance evaluation. *Electronics*. 2020. Vol. 9, No. 8. Article 1295. DOI: https://doi.org/10.3390/electronics9081295.

98. MacQueen J. Some methods for classification and analysis of multivariate observations. In: Le Cam L. M., Neyman J. (eds.). *Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability*. Vol. 1. Berkeley: University of California Press, 1967. P. 281–297.

99. Ullah W., Muhammad Y., Uddin I., Chong K. P. K-means clustering on noisy intermediate scale quantum computers. *arXiv preprint* arXiv:1909.12183. 2019. URL: https://arxiv.org/abs/1909.12183.

100. Satopaa V., Albrecht J., Irwin D., Raghavan B. Finding a “Kneedle” in a haystack: Detecting knee points in system behavior. In: *Proceedings of the 31st International Conference on Distributed Computing Systems Workshops*. 2011. P. 166–171. DOI: https://doi.org/10.1109/ICDCSW.2011.

101. Jolliffe I. T., Cadima J. Principal component analysis: A review and recent developments. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*. 2016. Vol. 374, No. 2065. Article 20150202. DOI: https://doi.org/10.1098/rsta.2015.0202.

102. Kleis S., Rueckmann M., Schaeffer C. G. Continuous-variable quantum key distribution with a real local oscillator and without auxiliary signals. *arXiv preprint* arXiv:1908.03625. 2019. URL: https://arxiv.org/abs/1908.03625.

103. Korzh B., Lunghi T., Houlmann R., Zbinden H. Free-running InGaAs single photon detector with 1 GHz count rate. *Applied Physics Letters*. 2013. Vol. 104, No. 8. Article 081108. DOI: https://doi.org/10.1063/1.4866582.

104. Ludwick K. J. The signal-to-noise ratio for photon counting after photometric corrections. *arXiv preprint* arXiv:2203.16501. 2024. DOI: https://doi.org/10.48550/arXiv.2203.16501.

105. Baek B., Hadfield R. H., Nam S. W., Kim J. Timing jitter of superconducting nanowire single-photon detectors. *Applied Physics Letters*. 2009. Vol. 95, No. 19. Article 191110. DOI: https://doi.org/10.1063/1.3264083.

106. Huang D., Lin D., Wang C., Liu W., Fang S., Liang C., Zeng G. Field demonstration of a continuous-variable quantum key distribution network. *Scientific Reports*. 2016. Vol. 6. Article 19201. DOI: https://doi.org/10.1038/srep19201.

107. Зінченко, В. Л., & Захожай, О. І. (2025, 26 березня). Інформаційна модель виявлення та класифікації атак у квантових каналах зв'язку на основі кластерного аналізу [Тези доповіді]. Innovative Approaches in Modern Science and Technology (Lisbon, Portugal). С. 116–117.

108. Yu F. X., Choromanski K., Kumar S., Jebara T., Chang S.-F. On learning from label proportions. *arXiv preprint* arXiv:1402.5902. 2014. DOI: https://doi.org/10.48550/arXiv.1402.5902.

109. Liu F., Chen L., Zheng Y., Feng Y. A prediction method with data leakage suppression for time series. *Electronics*. 2022. Vol. 11, No. 22. Article 3701. DOI: https://doi.org/10.3390/electronics11223701.

110. Yang X., et al. Research on information leakage in time series prediction. *Scientific Reports*. 2024. Vol. 14. Article 80018. DOI: https://doi.org/10.1038/s41598-024-80018-9.

111. Talagala T. S., et al. tsdataleaks: An R package to detect potential data leaks in forecasting competitions. *arXiv preprint* arXiv:2402.10522. 2024. URL: https://arxiv.org/abs/2402.10522.

112. Liu F., Chen L., Zheng Y., Feng Y. A prediction method with data leakage suppression for time series. *Electronics*. 2022. Vol. 11, No. 22. P. 3701. DOI: https://doi.org/10.3390/electronics11223701.

113. He K., Zhang X., Ren S., Sun J. Delving deep into rectifiers: Surpassing human-level performance on ImageNet classification. In: *Proceedings of the IEEE International Conference on Computer Vision (ICCV)*. 2015. P. 1026–1034. DOI: https://doi.org/10.1109/ICCV.2015.123.

114. Kingma D. P., Ba J. Adam: A method for stochastic optimization. *arXiv preprint* arXiv:1412.6980. 2015. DOI: https://doi.org/10.48550/arXiv.1412.6980.

115. Зінченко, В. Л., & Лифар, В. О. (2024, жовтня). Використання нейронних мереж для оптимізації квантових каналів зв'язку у квантовій криптографії. У Матеріали науково-практичної конференції з інформаційних технологій (м. Миколаїв, Україна). Інформаційні технології: моделі, алгоритми, системи (ITMAS – 2024). С 102-103.

ДОДАТКИ

Додаток А

Документи, що підтверджують впровадження результатів дисертації

АТі

ТОВ "АЙТІ-РІШЕННЯ"
04050, м. Київ, вул. Студентська, 3

АКТ

впровадження результатів наукових досліджень Зінченка В.Л.
на тему: «Інформаційна технологія підтримки рішень в захищеній системі квантової передачі інформації»

Компанія ТОВ «АЙТІ-РІШЕННЯ» на основі аналізу технічних рішень, запропонованих в дисертаційній роботі В.Л. Зінченка, встановила наступне.

Результати дослідження спрямовані на створення інструментарію для оцінки та управління станом квантових каналів зв'язку.

Запропоновані математичні моделі, алгоритми та програмні засоби забезпечують можливість кількісного аналізу параметрів квантових потоків, формування критеріїв прийняття рішень та підвищення ефективності заходів із захисту інформації.

Використання отриманих результатів дозволяє реалізувати сучасні підходи до моніторингу інформаційних потоків із застосуванням нейронних мереж і визначати вимоги до технічних засобів контролю та реагування у системах захищеної передачі даних.

Директор департаменту технічного **Іван ЗІМІН**

«ЗАТВЕРДЖУЮ»

Ректор Східноукраїнського
національного
університету імені Володимира Даля
_____ О.В. Поркуян
«____» _____20 __ р.

АКТ

про впровадження в освітній процес результатів дисертаційної роботи
Зінченка Володимира Леонідовича
за напрямом: «Інформаційна технологія підтримки рішень в захищеній системі квантової передачі інформації»,
представленої на здобуття наукового ступеня доктора філософії

Цим актом підтверджується, що результати досліджень Зінченка В.Л., які проводилися за науковим напрямом «Інформаційна технологія підтримки рішень в захищеній системі квантової передачі інформації», впроваджені в освітній процес на кафедрі інформаційних технологій та програмування Східноукраїнського національного університету імені Володимира Даля при підготовці фахівців другого (магістерського) рівня вищої освіти за спеціальністю 126 «Інформаційні системи і технології», освітня програма «Інформаційні системи та технології», зокрема

- розглядається інформаційна технологія підтримки рішень для захищеної квантової передачі інформації;

- використано результати розробки нейронних мереж та алгоритмів кластеризації для автоматичного виявлення аномалій у потоках даних;

Результати інтегровані в освітні компоненти «Інформаційна безпека та управління ризиком», «Інформаційні технології комп'ютерних мереж», а також при підготовці магістерських досліджень.

Узгоджено:

Завідувач кафедри інформаційних технологій
та програмування Східноукраїнського національного
університету імені Володимира Даля,
д.т.н., професор О.І. Захожай

Додаток Б

Приклади реалізації модулів інформаційної технології для контролю, класифікації, та забезпечення достовірності інформації, у квантових каналах зв'язку

Модуль PDA (Мовою Python)

```
from dataclasses import dataclass
from typing import Tuple
import numpy as np

EPS = 1e-12

@dataclass
class PDA:
    L: int
    def compute_features(self, series_matrix: np.ndarray) -> Tuple[np.ndarray,
np.ndarray]:
        assert series_matrix.ndim==2 and series_matrix.shape[1]==self.L
        means = series_matrix.mean(axis=1)
        stds  = series_matrix.std(axis=1, ddof=0)
        mins  = series_matrix.min(axis=1)
        maxs  = series_matrix.max(axis=1)
        cvs   = stds/(np.abs(means)+EPS)
        fbm = np.column_stack([means, stds, mins, maxs, cvs])
        return fbm, means
```

Модуль PDA (Мовою Python)

```
from dataclasses import dataclass
import numpy as np

@dataclass
class FBMBuilder:
    def build(self, features_matrix: np.ndarray) -> np.ndarray:
        return features_matrix
```

Модуль NFBM (Мовою Python)

```
from dataclasses import dataclass, field
import numpy as np
EPS = 1e-12

@dataclass
class NFMB:
    mins: np.ndarray = field(default=None)
    maxs: np.ndarray = field(default=None)

    def fit(self, fbm_list):
        stacked = np.vstack(fbm_list)
        self.mins = stacked.min(axis=0)
        self.maxs = stacked.max(axis=0)

    def transform(self, fbm: np.ndarray)->np.ndarray:
        assert self.mins is not None and self.maxs is not None
        denom = (self.maxs - self.mins) + EPS
        return (fbm - self.mins)/denom

    def fit_transform(self, fbm_list):
        self.fit(fbm_list)
        return [self.transform(f) for f in fbm_list]
```

Модуль NN (Мовою Python)

```
from dataclasses import dataclass
from typing import Tuple
import numpy as np

LABELS = {0: "stationary", 1: "anomaly"}
def sigmoid(z): return 1.0/(1.0+np.exp(-z))

@dataclass
class OnlineLogisticNN:
    input_dim: int
    lr: float = 0.05
    w: np.ndarray = None
    b: float = 0.0
    supports_training: bool = True

    def __post_init__(self):
        if self.w is None:
```

```
            rng = np.random.default_rng(42)
            self.w = rng.normal(0, 0.01, size=self.input_dim).astype(float)

    def predict_proba(self, x: np.ndarray)->float:
        z = float(np.dot(self.w, x) + self.b); return sigmoid(z)

    def predict(self, x: np.ndarray)->Tuple[int, str, float]:
        p = self.predict_proba(x); y_hat = 1 if p >= 0.5 else 0; return y_hat,
LABELS[y_hat], p

    def update(self, x: np.ndarray, y: int, epochs: int = 1):
        for _ in range(epochs):
            p = self.predict_proba(x)
            grad = (p - y)
            self.w -= self.lr * grad * x
            self.b -= self.lr * grad

# MATLAB integration
try:
    import matlab.engine as _mlab_eng  # type: ignore
    _MATLAB_AVAILABLE = True
except Exception:
    _mlab_eng = None
    _MATLAB_AVAILABLE = False

@dataclass
class MatlabNN:
    input_dim: int
    func_predict: str = "qkd_model_predict"
    func_train: str = ""      # optional
    threshold: float = 0.5
    start_engine: bool = True
    matlab_path: str = ""
    startup_script: str = ""
    eng: any = None
    supports_training: bool = False

    def __post_init__(self):
        if not _MATLAB_AVAILABLE:
            raise ImportError("MATLAB Engine for Python недоступний. Встановіть
engine: <MATLABROOT>/extern/engines/python -> pip install .")
        if self.start_engine or self.eng is None:
            self.eng = _mlab_eng.start_matlab()
        if self.matlab_path:
            self.eng.addpath(self.matlab_path, nargout=0)
        if self.startup_script:
            self.eng.eval(self.startup_script, nargout=0)
        self.supports_training = bool(self.func_train)
```

```
    def _to_mat(self, x):
        x = np.asarray(x, dtype=float).reshape(1, -1)
        return self.eng.double(x.tolist())

    def predict_proba(self, x):
        xm = self._to_mat(x)
        try:
            label, p = self.eng.feval(self.func_predict, xm, nargout=2)
            p = float(p[0][0]) if hasattr(p, "__len__") else float(p)
            return p
        except Exception:
            p = self.eng.feval(self.func_predict, xm, nargout=1)
            p = float(p[0][0]) if hasattr(p, "__len__") else float(p)
            return p

    def predict(self, x):
        p = self.predict_proba(x)
        y_hat = 1 if p >= self.threshold else 0
        return y_hat, LABELS[y_hat], p

    def update(self, x, y, epochs:int=1):
        if self.func_train:
            xm = self._to_mat(x)
            self.eng.feval(self.func_train, xm, float(y), int(epochs), nargout=0)
        return
```

Модуль DCM (Мовою Python)

```
from dataclasses import dataclass
@dataclass
class DCM:
    anomaly_policy: str = "continue"
    def act(self, y_label: str)->str:
        if y_label == "anomaly" and self.anomaly_policy=="halt_on_anomaly":
            return "HALT"
        return "CONTINUE"
```

Модуль FBM (Мовою Python)

```
from dataclasses import dataclass, field
from typing import List
@dataclass
class SCM:
    y_preds: List[str] = field(default_factory=list)
    def record(self, y_label: str): self.y_preds.append(y_label)
    def sequence(self)->List[str]: return list(self.y_preds)
```

Модуль NFBM (Мовою Python)

```
from dataclasses import dataclass
from typing import Dict, List, Tuple
from collections import Counter

@dataclass
class MajorityVotePA:
    tie_break: str = "anomaly"
    def decide(self, y_seq: List[str])->Tuple[str, Dict[str, int]]:
        if not y_seq: return "stationary", {"stationary":0, "anomaly":0}
        c = Counter(y_seq)
        if c.get("anomaly",0) == c.get("stationary",0):
            return self.tie_break, dict(c)
        lab = max(c.items(), key=lambda kv: kv[1])[0]
        return lab, dict(c)
```

ДОДАТОК В

Результати виконання модуля РА

30 – серій, кожна складає 100 вимірювань з одного датчиків, кількість датчиків – 5.

```
C:\Users\User\Desktop\qkd_model> python main.py --sensors 5 --L 100 --calib 5 --series 30 --policy continue
[РА] ПІДСУМКИ БІЛЬШОСТІ:
    Класифіковано серій: 30
    Лічильники: {'stationary': 27, 'anomaly': 3}
    Остаточний клас каналу: stationary
```

30 – серій, кожна складає 100 вимірювань з одного датчиків, кількість датчиків – 5.

```
[РА] ПІДСУМКИ БІЛЬШОСТІ:
    Класифіковано серій: 30
    Лічильники: {'stationary': 24, 'anomaly': 6}
    Остаточний клас каналу: stationary
```

30 – серій, кожна складає 100 вимірювань з одного датчиків, кількість датчиків – 5.

```
[РА] ПІДСУМКИ БІЛЬШОСТІ:
    Класифіковано серій: 30
    Лічильники: {'stationary': 12, 'anomaly': 18}
    Остаточний клас каналу: anomaly
```