UDC 621.391:530.145; 004.1; 004.4
SCOPUS CODE 1700
https://doi.org/10.36073/1512-0996-2025-4-102-112

კვანტური სიგნალის მუშაობის ტექნიკური ანალიზი პრაქტიკული ექსპერიმენტის ფარგლებში

მარიამ ჯანელიძე ციფრული სატელეკომუნიკაციო ტექნოლოგიების დეპარტამენტი, საქართველოს ტექნიკური უნივერსიტეტი, საქართველო, 0160, თბილისი, მ. კოსტავას 77
E-mail: mariamjanelidze100@gmail.com

ლაშა ჯანელიძე ციფრული სატელეკომუნიკაციო ტექნოლოგიების დეპარტამენტი, საქართველოს ტექნიკური უნივერსიტეტი, საქართველო, 0160, თბილისი, მ. კოსტავას 77
E-mail: lashajanelidze100@gmail.com

რეცენზენტები:

მ. ტაბატაძე, სტუ-ის ინფორმატიკისა და მართვის სისტემების ფაკულტეტის ასოცირებული პროფესორი
E-mail: m.tabatadze@gtu.ge

ნ. აბზიანიძე, სტუ-ის ინფორმატიკისა და მართვის სისტემების ფაკულტეტის ასოცირებული პროფესორი
E-mail: n.abzianidze@gtu.ge

ანოტაცია. ციფრული ეპოქის სწრაფი განვითარება და ინფორმაციული ტექნოლოგიების მზარდი მოთხოვნები აჩენს საჭიროებას შეიქმნას. უფრო საიმედო, უსაფრთხო და ეფექტური საკომუნიკაციო სისტემები ამ კონტექსტში, კვანტური სიგნალები წარმოადგენს მომავლის ტექნოლოგიას, რომელიც პასუხობს იმ გამოწვევებს, რასაც კლასიკური სიგნალების სისტემები ვეღარ უმკლავდებიან — მაგალითად, ინფორმაციის უმაღლესი დონის დაცულობა, სიზუსტე და გადაცემის სიჩქარე. კვანტური ჩახლართულობის, სუპერპოზიციისა და კორელაციების გამოყენება შესაძლებელს ხდის ინფორმაციის უმაღლეს დონეზე დაცვას და დამუშავებას. შესაბამისად, კვანტური სიგნალების დანერგვა კრიტიკულად მნიშვნელოვანია ისეთი სფეროებისთვის, როგორიცაა კვანტური კავშირი, უსაფრთხო კიბერინფრასტრუქტურა, მაღალტექნოლოგიური სენსორიკა და კვანტური გამოთვლითი სისტემები. ნაშრომში მიმოხილულია კვანტური სიგნალების როლი თანამედროვე ტექნოლოგიებში და მათი პოტენციალი უახლოეს მომავალში. კვანტური სიგნალების

თეორია აერთიანებს კვანტური ფიზიკის, ინფორმაციის თეორიისა და სიგნალების დამუშავების პრინციპებს. ეს მახასიათებლები უზრუნველყოფს ინფორმაციის გადაცემას და დამუშავებას უმაღლესი სიზუსტით, რაც განსაკუთრებით მნიშვნელოვანია კვანტური კავშირის, კვანტური რადარებისა და კვანტური სენსორიკის განვითარებაში. მოცემულ ნაშრომში მიმოიხილება კვანტური სიგნალების თეორიული საფუძვლები, ძირითადი მოდელები და მათი პოტენციური გამოყენება თანამედროვე ტექნოლოგიებში.

საკვანძო სიტყვები: ბლოქს-ბენის მეთოდი; კვანტური სიგნალი; კვანტური თეორია; კვანტური ჩახლართულობა; კუბიტები; კვანტური სუპერპოზიცია; კვანტური ტელეპორტაცია; კვანტური მდგომარეობა; კვანტური ინტერნეტი; კვანტური მექანიკა; კრიფტოგრაფიული გასაღები; პოლარიზაცია; პროტოკოლი BB84; ფოტონი.

შესავალი

კვანტური სიგნალების ფენომენი სერიოზულად არის დაკავშირებული კვანტური ფიზიკის განვითარებასთან, რომლის დასაწყისი XIX საუკუნის ბოლოსა და XX საუკუნის დასაწყისშია. კვანტური ფიზიკის ფუნდამენტური პრინციპების აღმოჩენა, როგორიცაა ენერგიის კვანტიზაცია, ინტეგრირებული იყო სიგნალების გაშიფვრისა და დამუშავების პოტენციურ კონცეფციებში. კვანტური თეორიის პირველი საფუძვლები ჩაყრილი იყო უკვე 1900 წელს, როდესაც მაქს პლანკმა გამოთქვა ენერგიის კვანტიზაციის კონცეფცია. მისი თეორია სინათლის გამოსხივებას ეყრდნობოდა, თუმცა ამით მან დიდი შთაგონება მისცა მომავალ კვლევებს კვანტური სიგნალების შესახებ. ვერზენის მუშაობამ (1913) ე.წ. „ატომის სიგნალები“ გამოაცოცხლა, უფრო კონკრეტულად საუბარია, ელექტრონების მოძრაობაზე ატომში და მის გავლენაზე გამოსხივების ხასიათზე. კვანტური ფიზიკის ზრდის პარალელურად, 1935 წელს აინშტაინმა და პოდოლსკიმ წამოაყენეს ცნობილი "EPR პარადოქსი", რომელიც ყურადღებას ამახვილებდა კვანტური ჩახლართულობის ფენომენზე — მდგომარეობა, სადაც ორ ნაწილაკს შორის არსებობდა ისეთი შეზღუდული კავშირი, რომ ერთის მდგომარეობა განსაზღვრავდა მეორისას, მიუხედავად მათი დაშორებისა. ამის შემდგომ XX ს-ის 60–70-იან წლებში შეიქმნა კვანტური ინფორმაციის თეორიის კონცეფცია. შორეული პრინციპები, როგორიცაა კუბიტები და კვანტური ტელეპორტაცია, მჭიდროდ იყო დაკავშირებული კვანტური სიგნალების დასაბუთების ამ ეტაპზე. ამის შემდგომ კვანტური კოდირება და კომუნიკაცია ხდება აქტუალური თემები, რასაც მოგვიანებით მივყავართ კვანტური კომუნიკაციის სისტემების წამოწყებამდე. XX ს-ის 90-იანი წლების ბოლოს და 2000-იანი წლების დასაწყისში კვანტური სიგნალების თეორია მოექცა ფართო სამეცნიერო ინტერესების ცენტრში. კვანტური კომპიუტერების, კვანტური რადარებისა და კვანტური კომუნიკაციის წინსვლამ რეალურად გამოავლინა მათი პოტენციალი არა მხოლოდ აკადემიურ სფეროში, არამედ შუალედური ტექნოლოგიების განვითარებაშიც. დღეს, კვანტური სიგნალები ინტეგრირებულია ისეთ პროექტებში, როგორიცაა კვანტური ინტერნეტი, კვანტური კრიპტოგრაფია და კვანტური სენსორიკა. კვანტური სიგნალების

თანამედროვე თეორია ეფუძნება კვანტური მექანიკის პრინციპებს და წარმოადგენს ინტერდისციპლინურ სფეროს, რომელიც დაკავშირებულია სიგნალების დამუშავებასთან, კვანტური ინფორმაციის თეორიასა და კვანტური ტექნოლოგიების განვითარებასთან. ეს თეორია არ ამარტივებს მხოლოდ ინფორმაციის გადაცემის კლასიკურ პრინციპებს, არამედ გვთავაზობს ახალ გზებს, როგორიცაა სიგნალების კვანტური მექანიზმები, რომლებიც საშუალებას იძლევა ინფორმაციის გადაცემა და დამუშავება ბევრად უფრო ეფექტურად და უსაფრთხოდ მოხდეს. კვანტური სიგნალების თეორია არის კვანტური მექანიკის გამოყენება სიგნალების გადაცემისას, რომელიც მოიცავს არა მხოლოდ კლასიკურ სიგნალებს (როგორიცაა ელექტრომაგნიტური ტალღები), არამედ ახალ მახასიათებლებს, როგორიცაა: კვანტური ჩახლართულობა, სუპერპოზიცია, არაინტუიციური კორელაციები. განვიხილოთ თითოეული მათგანი. კვანტური ჩახლართულობა არის ფენომენი, რომელშიც ორი და მეტი ნაწილაკი სიგნალების გადაცემისას ისე იწევენ ერთმანეთისკენ, რომ ერთი ნაწილაკის მდგომარეობა განსაზღვრავს მეორისას, მიუხედავად მათი დაშორებისა. ამ პრინციპით სიგნალები უფრო უსაფრთხო და ეფექტურია, რადგან ინფორმაციის გამჟღავნება შეიძლება მხოლოდ სპეციალურად დაშიფრული სისტემის მეშვეობით. ასევე კვანტური სიგნალები შეიძლება არსებობდნენ ერთდროულად სხვადასხვა მდგომარეობაში, რაც მათ საშუალებას აძლევს, რომ პარალელურად გადაიცეს უფრო დიდი მონაცემების ნაკადი. სწორედ ამ სხვადასხვა მდგომარეობას ვუწოდებთ სუპერპოზიციას. ამასთანავე, აუცილებელია შევეხოთ არაინტუიციურ კორელაციებს, მათი პრაქტიკული მნიშვნელობა კი შემდეგია: კვანტური სიგნალები იყენებენ სპეციალურ კორელაციებს, რომლებიც კლასიკური ინფორმაციული სისტემებისთვის არაა ხელმისაწვდომი, რაც უზრუნველყოფს მაღალ დონეზე ეფექტურობას და საიმედოობას. რა თქმა უნდა, კვანტური სიგნალების გამოყენება წარმოუდგენელია კვანტური კომუნიკაციის სრულყოფილი სისტემის გარეშე. სწორედ კვანტური კომუნიკაცია წარმოადგენს თანამედროვე კვანტური სიგნალების ერთ-ერთ ძირითად მიმართულებას. ამ შემთხვევაში, კვანტური სიგნალები გამოყენებულია ინფორმაციის უსაფრთხოებისა და გამძლეობისთვის. კვანტური კრიპტოგრაფია და კვანტური კვალიფიცირებული კოდირება გამოიყენება ინფორმაციის დაცვისთვის, რაც ამცირებს გაჟონვის რისკს. კვანტური ინტერნეტი ითვალისწინებს კვანტური სიგნალების გამოყენებას ქსელურ სიგნალებში, რაც მნიშვნელოვნად ზრდის სისტემის სიჩქარეს, უსაფრთხოებას და ინტერნეტის სტაბილურობას

ძირითადი ნაწილი

კვანტური სიგნალის მუშაობის სისტემა ეფუძნება კვანტურ მექანიკას და კვანტური ფიზიკის უმნიშვნელოვანეს პრინციპებს, როგორიცაა კვანტური ჩახლართულობა (Entanglement), სუპერპოზიცია, და კვანტური მასობრივი შიფრაცია. ეს პრინციპები ქმნის საფუძველს ინფორმაციის გადაცემისთვის სრულიად ახალ სისტემაზე, რომელიც გაცილებით უსაფრთხო და დაცულია ტრადიციული საკომუნიკაციო სისტემებისგან. განვიხილოთ, თუ როგორ

მუშაობს კვანტური სიგნალი და მისი ძირითადი პრინციპები. მაგალითად. თუ ჩვენ ციფრულ ინფორმაციას აღვიქვამთ როგორც 0 და 1 ისინი ჩვეულებრივ ცალ-ცალკე არსებობენ. კვანტური სისტემის შემთხვევაში, ფოტონი შეიძლება იყოს 0-შიც და 1-შიც ერთდროულად, რაც მას უზარმაზარ შესაძლებლობებს ანიჭებს მონაცემების გადაცემისა და დამუშავებისას. აუცილებელია განვიხილოთ კვანტური გაუქმებლობა (Entanglement), რომელიც გულისხმობს ორ კვანტურ ნაწილაკებს შორის სპეციალურ კავშირს, როდესაც თითოეული ნაწილაკი ვითარდება ისე, რომ მისი მდგომარეობა მთლიანად დამოკიდებულია სხვა ნაწილაკის მდგომარეობაზე, მიუხედავად იმისა, რამდენად შორს არიან ისინი ერთმანეთისგან. ეს ფენომენი, როგორც წესი, ხდება მხოლოდ მაშინ, როცა ნაწილაკები ერთდროულად არიან დაკავშირებულნი. პრაქტიკული მაგალითის სახით რომ ვთქვათ, ორი ფოტონი, რომლებიც განიცდიან ჩახლართულობას, ერთდროულად შეცვლიან თავიანთ მდგომარეობას, მიუხედავად იმისა, თუ რამდენი კილომეტრია დაშორება მათ შორის. თუ ერთი ფოტონის მდგომარეობა შეიცვლება (მაგალითად, მისი პოლარიზაცია შეიცვლება), მეორე ფოტონი ამ მდგომარეობაზე იმოქმედებს გეომეტრიულად. აუცილებელია აღინიშნოს კვანტური კომუნიკაცის ერთ-ერთი ყველაზე მნიშვნელოვანი კომპონენტი კვანტური გასაღების განაწილება (Quantum Key Distribution (QKD)- ი). ეს მეთოდი უზრუნველყოფს უსაფრთხო მონაცემთა გადაცემას, რადგან ნებისმიერი ჩარევა ან ციფრულ მონაცემებში შეცვლა, რომელიც ხდება კვანტურ სისტემაში ჩარევით, ცვლილებებს იწვევს თავად სიგნალის ანალიზში. ეს მექანიზმი აფერხებს მესამე მხარის მიერ მონაცემების მოპარვას. სწორედ ეს არის მეთოდი, რომელიც გამოიყენება უსაფრთხო კომუნიკაციების უზრუნველსაყოფად კვანტური კომუნიკაციის ტექნოლოგიაში. ეს მეთოდი საშუალებას აძლევს ორ მხარსე (მაგალითად, ორი მომხმარებელი) უსაფრთხოდ გააზიარონ კრიპტოგრაფიული გასაღები, რომელიც გამოიყენება ინფორმაციის დაშიფვრისა და მისი დეკოდირებისთვის. კვანტური გასაღების განაწილების ერთ-ერთი ძირითადი პრინციპია, რომ კვანტური ინფორმაციის გადაცემა ხელს უშლის მესამე მხარის ჩარევას.

კვანტურ მდგომარეობებში ფოტონები ძალიან მგრძნობიარენი არიან გარე ცვლილებების მიმართ და თუ რომელიმე მხარე ეცდება სიგნალის გაშიფვრას ან მის ცვლილებას, კვანტური მდგომარეობა დაუყოვნებლივ შეიცვლება. შესაბამისად ყოველგვარი გარე ჩარევისას მოხდება ინფორმაციის დამახინჯება, რაც გვაძლევს იმის გარანტიას, რომ მხარე რომელიც ინფორმაციის მოპარვას ცდილობს, ინფორმაციას ვერ მიიღებს და ამასთანავე ჩარევის მცდელობა გასაღების მქონე (გამგზავნი და მიმღები) მხარეებისთვის გახდება ცნობილი.

როგორც უკვე ვთქვით, კვანტური გასაღების მქონე მხარეებს (გამგზავნი და მიმღები) შეუძლიათ, განსაზღვრონ, კვანტურ სიგნალზე მოხდა თუ არა გარე ჩარევა. ამისთვის გამოიყენება ეგრეთ წოდებული „Bismarck“-ის (ბისმარკ/ბენედიქტის) მეთოდი, რომლის მიხედვითაც, გასაღების განაწილების პროცესში მხარეები ერთმანეთს უგზავნიან სიგნალების მონაცემებს და შედარების შედეგებს, რათა შეამოწმონ, მოხდა თუ არა სიგნალზე მანიპულაცია.

ამ მეთოდის გამოყენებით, როდესაც ორი მხარე ცდილობს გასაღების განაწილებას, ისინი ერთმა-

ნეთს სიგნალების მონაცემებს და შედარების შედეგებს უგზავნიან. თუ მათ შორის ერთ-ერთი ფოტონი შეცვლილია, მხარეები ადვილად აღმოაჩენენ, რომ მესამე მხარის ჩარევა მოხდა. კვანტური სიგნალების გადაცემის ტექნიკური ანალიზისას აუცილებელია განვიხილოთ BB84 მეთოდი, სწორედ ის წარმოადგენს პირველი კვანტური გასაღების განაწილების პროტოკოლს, რომელიც იყენებს კვანტურ პოლარიზაციებს, რათა უსაფრთხოდ გადაანაწილოს გასაღები და უზრუნველყოს მონაცემების დაცვა. ამ მეთოდის მეშვეობით შესაძლებელი გახდა კლასიკური ინფორმაციის გადაცემა ისე, რომ ნებისმიერი ჩარევა თუ ჩარევის მცდელობა გამხდარიყო შესამჩნევი. BB84 ერთ-ერთი მთავარი ალგორითმია კვანტური კომუნიკაციისა და კვანტური შიფრაციის სისტემებში. BB84 მეთოდში მონაცემთა გადაცემას უსაფრთხო და საიმედო გზით უზრუნველყოფს კვანტური სისტემის ის პრინციპები, რომლებიც კლასიკური სისტემებისგან განსხვავებულია. ეს მეთოდი ეფუძნება რამდენიმე მყარ კონცეფციას, მათ შორის BB84 პოლარიზაციის მექანიზმს, რომელიც იყენებს კვანტური ფიზიკის პრინციპებს. აღნიშნული ეხება ფოტონების პოლარიზაციას. პოლარიზაცია მიუთითებს ფოტონის ტალღის მიმართულებას, რომელიც შეიძლება იყოს სხვადასხვა ხარისხში და მიმართულებით. BB84-ში იყენებენ ორ პოლარიზაციის ბაზას, კერძოდ ჰორიზონტალურს/ვერტიკალურს (0° და 90°), და დიაგონალურს (45° და 135°). როდესაც ფოტონები გადაეცემა ერთ ბიტს (0 ან 1), ისინი ინახავენ კონკრეტულ პოლარიზაციას, რაც შესაძლებელია გამოყენებული იქნეს როგორც გასაღების მექანიზმი. BB84 მეთოდის ძირითადი პროცესი, რომელიც ემყარება კვანტურ პოლარიზაციებს, შეიძლება განისაზღვროს რამდენიმე მარტივი ნაბიჯით, ერთ-ერთია, კომუნიკატორების არჩევანი და ფოტონების გაგზავნა. თავდაპირველად ორი კომუნიკატორი (A და B) ერთმანეთს ეკონტაქტება და გადაწყვეტენ, რომ დაიწყებენ კვანტური გასაღების განაწილების პროცესს. A მხარე (გამგზავნი) შემთხვევით არჩევს ერთ-ერთს იმ ოთხივე პოლარიზაციიდან (ჰორიზონტალური, ვერტიკალური, დიაგონალური და მისი ინვერსიები) თითოეული ფოტონის გადაცემის დროს. თითოეულ ფოტონს მიენიჭება ორი ბიტი (0 ან 1) და გადაეცემა მეორე მხარეს (B).

შემდეგი ნაბიჯი, რა თქმა უნდა, არის მიღება და გაზომვა. მეორე მხარე (B) იღებს ფოტონებს და მიმართავს მათ, თავის პოლარიზაციის ბაზას, რათა აირჩიოს, როგორ შეადაროს და მიუსადაგოს თითოეული ფოტონი.

მას შეუძლია შეარჩიოს ჰორიზონტალური/ვერტიკალური ან დიაგონალური პოლარიზაციის ბაზა. არსებობს შანსი, რომ B-მ აირჩიოს ზუსტად ის ბაზა, რაც A-მ გამოიყენა, მაგრამ შანსი ასევე არსებობს, რომ ისინი გაატარებენ სხვადასხვა ბაზებს, რაც გამოიწვევს შეცდომას. შემდგომი ეტაპია გადასაცემი ფოტონების შედარება, კერძოდ, როცა ორივე მხარე (A და B) იღებს საკუთარ მონაცემებს, ისინი მიმართავენ ერთმანეთს და შედარებით აღმოაჩენენ, თუ რომელი ფოტონები იყო გადაცემული იმავე პოლარიზაციის ბაზებით. როდესაც ისინი შეთანხმდებიან, რომელი პოლარიზაციები იყო სწორი, ამ ფოტონების მიხედვით ხდება გასაღების შექმნა. რა თქმა უნდა, უმნიშვნელოვანესი ფაქტორია შეცდო-

მების აღმოფხვრა და გასაღების კონფიდენციალურობის უზრუნველყოფა. კერძოდ, თუ არსებობს შეცდომები (ამ შემთხვევაში, თუ A-ს და B-ს შორის პოლარიზაციის ბაზები განსხვავდება), ისინი არ აპირებენ მათ გამოყენებას გასაღების შექმნაში. ამაზე დაყრდნობით ორივე მხარე მოიპოვებს სასურველ უსაფრთხო გასაღებს. გარდა ზემოთ განხილულისა, BB84-ის ერთ-ერთი მთავარი უპირატესობა არის ის, რომ მას შეუძლია ადვილად აღმოაჩინოს ნებისმიერი მესამე პირის ჩარევა. თუ მესამე პირი ცდილობს ჩარევას, და მას არ ექნება ხელთ სრულყოფილი პოლარიზაციის ინფორმაცია, ის აუცილებლად გამოიწვევს შეცდომას. ეს პროცესი ქმნის უსაფრთხო გარემოს, სადაც კომუნიკაციის კონფიდენციალურობა სერიოზულად არის დაცული. BB84 პროტოკოლი აღიარებულია მსოფლიოში ყველაზე უსაფრთხო კვანტური გასაღების განაწილების მეთოდად. აღნიშნულზე შეჯამების სახით შეგვიძლია ვთქვათ, რომ ბლოქს-ბენის მეთოდი (BB84) წარმოადგენს კვანტური გასაღების განაწილების ერთ-ერთ ყველაზე წარმატებულ და კარგად აპრობირებულ პროტოკოლს. მისი გამოყენებით შესაძლებელია კვანტური კომუნიკაციის სისტემების შექმნა, რომლებსაც შეუძლია უზრუნველყოს მონაცემების გადაცემის უსაფრთხოება ისე, რომ გარე პირებმა ვერ შეძლონ მათი მოპარვა. მიუხედავად ტექნოლოგიური გამოწვევებისა, BB84 წარმოადგენს კვანტური კრიპტოგრაფიის მძლავრ საყრდენ ბლოკს.

```python
from qiskit import QuantumCircuit, Aer, execute
qc = QuantumCircuit(1, 1)
qc.h(0)
qc.measure(0, 0)
simulator = Aer.get_backend('qasm_simulator')
result = execute(qc, simulator, shots=1).result()
measurement = result.get_counts(qc)
print(f"Measurement result: {measurement}")

```

პრაქიკული მაგალითისთვის IBM-ის კვანტური პროგრამირების ფრეიმვორკი გამოვიყენეთ. მოცემულ სიმულაციაში IBM-ის კვანტური პროგრამირების ფრეიმვორკი, Hadamard Gate კვანტური კავშირი იწყება სიგნალით, რაც ცვლის კვანტურ ბიტს (qubit) სუპერპოზიციაში. შემდეგ, ჩატარებულ კვალიფიკაციაში კუბიტი ზომავს, რის შემდეგაც მიიღება ან "0" ან "1". კვანტური სიმულატორი აჩვენებს, თუ რა შედეგი მიიღება შემთხვევითობის საფუძველზე. თუმცა შეგვიძლია ეს პროცესი უფრო განვავითაროთ. მეორე სიმულაციაში შედეგები გადმოსცემს შემთხვევით "0"-ს ან "1"-ს, რაც შეიძლება გამოიყენოს როგორც ერთ-ერთი კვანტური გასაღების bit-ი,

```python
from qiskit import QuantumCircuit, Aer, execute
import random
def bb84_protocol():
    alice_bits = [random.choice([0, 1]) for _ in range(4)]
    alice_bases = [random.choice(['+','x']) for _ in range(4)]
    print(f"Alice's Bits: {alice_bits}")
    print(f"Alice's Bases: {alice_bases}")

    bob_bases = [random.choice(['+','x']) for _ in range(4)]
    print(f"Bob's Bases: {bob_bases}")
    results = []
    for i in range(4):
        qc = QuantumCircuit(1, 1)
        if alice_bases[i] == '+':
            if alice_bits[i] == 0:
                qc.i(0)
            else:
                qc.x(0)  #
        else:
            if alice_bits[i] == 0:
                qc.h(0)
            else:
                qc.h(0)
                qc.x(0)

        if bob_bases[i] == '+':
            qc.measure(0, 0)
        else:
            qc.h(0)
        simulator = Aer.get_backend('qasm_simulator')
        result = execute(qc, simulator, shots=1).result()
        counts = result.get_counts()
        results.append(int(list(counts.keys())[0]))

    print(f"Bob's Results: {results}")
    key = []
    for i in range(4):
```

რომელთა საფუძველზე შემდეგი კოდის ჰაკერული დაცვა განხორციელდება.

```
            if alice_bases[i] == bob_bases[i]:
                key.append(alice_bits[i])
        print(f"Final Key: {key}")

bb84_protocol()
```

უფრო განვითარებული კვანტური პროტოკოლი: BB84 ბევრად უფრო რეალური მაგალითი BB84 პროტოკოლია, სადაც კვანტური ენის საშუალებით გადაცემული სიგნალები ადასტურებს უსაფრთხო კომუნიკაციას. მოცემულ კოდში Alice ქმნის შემთხვევით ბიტებს და ირჩევს შემთხვევით პოლარიზაციის ბაზებს (მაგალითად, '+' ან 'x'). Bob-ი მიიღებს გზავნილ სიგნალებს, მაგრამ ის შემთხვევით აირჩევს ზომვის ბაზებს. Bob-ს მისი სიგნალების გასაუმჯობესებლად შეუძლია შესაბამისი პოლარიზაციის მეთოდების გამოყენება. Alice და Bob-ი შეადარებენ, თუ რომელ ბაზებში იყვნენ თანხმობაში და საერთო საიდუმლო გასაღებად ქმნიან მხოლოდ იმ ადგილებში, სადაც მათი ბაზები ემთხვეოდა. კვანტური სიგნალების სისტემები მუშაობს არა მხოლოდ იმისთვის, რომ კომუნიკაცია იყოს დაცული, არამედ იმისთვისაც, რომ ინფორმაციის გადაცემისას გამოწვეული პრობლემები სწრაფად გამოავლინონ. ყოველივე ამის შედეგად ცალსახაა რომ, კვანტური კომუნიკაცია მნიშვნელოვნად განსხვავდება კლასიკური სისტემებისგან, რადგან მისი დაცვის დონე გაცილებით მაღალია, ნებისმიერი ძლიერი ორგანიზებული შეტევის შემთხვევაშიც კი, სისტემა შეიცვლის თავის მდგომარეობას. მნიშვნელოვანი თავისებურება, რომელიც კვანტური სიგნალების შიფრაციას სხვა ტიპის შიფრაციის სისტემებისგან გამოარჩევს, არის ჩარევის აღმოჩენის ძალიან ძლიერი უნარი. კლასიკური შიფრაციის მეთოდებში მონაცემები შეიძლება გაიპაროს ან მათზე შეიძლება განხორციელდეს შეტევა ისე, რომ შეცდომა არ დაფიქსირდეს. თუმცა, კვანტური შიფრაციის სისტემებში, ინფორმაციის მოპარვის ან შეცვლის ნებისმიერი მცდელობა გამოიწვევს ცვლილებებს შიფრირებულ სიგნალებში. კვანტური მდგომარეობების სენსიტიურობა ჩარევის მიმართ მას პირდაპირ აფიქსირებს. როდესაც ბოროტმოქმედი გარეშე პირი შეეცდება შეცვალოს ფოტონის მდგომარეობა, ამას მყის გამოავლენს კვანტური სისტემა, ვინაიდან კვანტური შეცდომის გამოვლენა (quantum error detection) ხდება ძალიან მგრძნობიარე. აუცილებელია განვიხილოთ კვანტური ტელეპორტაცია, კვანტური ტელეპორტაცია არის ფიზიკური პროცესი, რომელიც საშუალებას იძლევა ინფორმაციის გადაცემისა ერთი ადგილიდან მეორეში ისე, რომ მონაცემები გადამოწმდება და „კოპირდება“ ერთ ადგილას, ხოლო მეორე ადგილას მისი ზუსტი ასლი იგზავნება, ამ პროცესის დროს ფიზიკური სიგნალი, როგორც წესი, არ გადადის სიგნალის წყაროდან დანიშნულების ადგილამდე, რაც მას რადიკალურად განასხვავებს კლასიკური ტელეპორტაციის ან ინფორმაციის გადაცემის სხვა მეთოდებისგან. კვანტური ტელეპორტაცია წარმოგვიდგება ისეთ პრაქტიკულ და თეორიულ მექანიზმად, რომელიც მნიშვნელოვნად ცვლის ინფორმაციის გადაცემის, კომპიუტერული და ინტერნეტსისტემების გამოყენებას. ამ ტექნოლოგიის სრულყოფის შემთხვევაში, ის შეიძლება გამოყენებული იქნეს არა მხოლოდ ინ-

ფორმაციის გადაცემაში, არამედ ახალი ტექნოლოგიების შესაქმნელად, მათ შორის ულტრაბგერითი კომუნიკაციების, კვანტური კრიპტოგრაფიისა და კვანტური ინტერნეტის შექმნისთვის. თუმცა, კვანტური ტელეპორტაცია ჯერ კიდევ დისტანციურ იდეად რჩება იმ მიზეზების გამო, რომ ამ ტექნოლოგიას აქვს მრავალი გამოწვევა, რომლებსაც სჭირდება ახალი კვანტური ოპტიკისა და ტექნოლოგიური ინოვაციების განვითარება. ერთ-ერთი ძირითადი გამოწვევა არის ის, რომ კვანტური ტელეპორტაციის მეთოდები ჯერ კიდევ საჭიროებს სპეციალურ მოწყობილობებს, რომლებიც ძალიან ძვირია თუმცა მათი სიზუსტე საკმაოდ მაღალია. მეცნიერები მუშაობენ ამ პრობლემების გადაჭრაზე და ცდილობენ, რომ ეს ტექნოლოგიები უფრო ხელმისაწვდომი და ეფექტური გახადონ. მიუხედავად ამისა, კვანტური ტელეპორტაცია ნამდვილად წარმოადგენს მომავლის ტექნოლოგიას, რომელმაც შესაძლოა გარდაქმნას ჩვენი კავშირი სამყაროსთან და საშუალებას მოგვცემს, რომ გადავლახოთ საელექტრონო კომუნიკაციებისა და ინფორმაციის გადაცემის არსებული შეზღუდვები. იმის გათვალისწინებით, რომ კვანტური ტელეპორტაცია მხოლოდ თეორიული კონცეფციაა, მისი რეალიზება წარმოადგენდეს არა მხოლოდ ტექნოლოგიური პრიორიტეტის სფეროს, არამედ მის შერჩევაში ჩართული გარემოებებისას. რა თქმა უნდა, როდესაც მეცნიერება მიაღწევს იმ დონეს, სადაც კვანტური ტელეპორტაცია რეალურად ხორციელდება, ის შეიძლება გახდეს ერთ-ერთი ყველაზე მნიშვნელოვანი მოვლენა კაცობრიობის ისტორიაში და ეს დაუყოვნებლივ გაამყარებს ახალ სტანდარტებს ტექნოლოგიაში, რომელიც გამოიყენება ყოველდღიურ ცხოვრებაში.

დასკვნა

კვანტური სიგნალის გადაცემის სისტემა წარმოადგენს ერთ-ერთ უმნიშვნელოვანეს ნაწილს კვანტური კომუნიკაციის განვითარებაში. მიუხედავად იმისა, რომ ტექნოლოგია ჯერ კიდევ საწყის ეტაპზეა და გარკვეული გამოწვევები არსებობს, აღნიშნული სისტემის უპირატესობები უსაფრთხოებისა და მონაცემთა საიდუმლოების თვალსაზრისით ძალზე შთამბეჭდავია. კვანტური სიგნალების შიფრაციის კიდევ ერთ ბრწყინვალე სამომავლო გამოყენებას წარმოადგენს კვანტური ინტერნეტი. ამასთან დაკავშირებით უკვე არსებობს პროექტები, რომლებშიც ცდილობენ შექმნან ისეთი კვანტური ქსელები, რომლებიც უზრუნველყოფენ არა მხოლოდ კომუნიკაციას, არამედ ყველა მონაცემის უსაფრთხოდ კოდირებას. კვანტური ინტერნეტი საშუალებას მისცემს მომხმარებლებს შეძლონ უკონტაქტო და უსაფრთხო ურთიერთობები ისე, რომ მათი ინფორმაციის უსაფრთხოება ყოველთვის დაცული იყოს. მიუხედავად ყველა გამოწვევისა, კვანტური სიგნალების შიფრაცია საკმაოდ წარმატებულია და შეიძლება საკმაოდ მალე გახდეს ჩვენი ყოველდღიური ცხოვრების ნაწილი. მისი უნიკალური თვისებები, როგორიცაა ჩარევის აღმოჩენა და მონაცემების სრული დაცვა, საშუალებას გვაძლევს, რომ ის გახდეს უსაფრთხოების ახალი სტანდარტი არა მარტო მეცნიერებაში, არამედ კიბერუსაფრთხოების სისტემებში, ფინანსურ ტრანზაქციებში თუ საჯარო და კერძო კომუნიკაციებში. მოცემულ კვლევაში ნათლად წარმოჩნდა, რომ კვანტური შიფრაცია უზრუნველყოფს მძლავრ უსაფრთხოებას, ამასთანავე დადგინდა, რომ ნებისმიერი გარე ჩარევა ამოცნობადია, რაც უზრუნველყოფს დაცულობის მაღალ დონეს.

ლიტერატურა

1. Scully, M. O., & Zubairy, M. S. (1997). *Quantum optics*. Cambridge University Press.
2. Sergienko, A. V. (2005). *Quantum communications and cryptography*. CRC Press.
3. Wiseman, H. M., & Milburn, G. J. (2009). *Quantum measurement and control*. Cambridge University Press.
4. Shankar, R. (1994). *Principles of quantum mechanics* (2nd ed.). Springer.
5. Wilde, M. M. (2017). *Quantum information theory* (2nd ed.). Cambridge University Press.
6. Zanardi, P., & Campos Venuti, L. (2007). *Quantum computation: A new paradigm*. Cambridge University Press.

UDC 621.391:530.145; 004.1; 004.4
SCOPUS CODE 1700
https://doi.org/10.36073/1512-0996-2025-4-102-112

Technical Analysis of Quantum Signal Performance in the Framework of Practical Experiments

Mariam Janelidze — Department of Digital Telecommunication Technologies, Georgian Technical University, Georgia, 0160, Tbilisi, 77, M. Kostava str.
E-mail: mariamjanelidze100@gmail.com

Lasha Janelidze — Department of Digital Telecommunication Technologies, Georgian Technical University, Georgia, 0160, Tbilisi, 77, M. Kostava str.
E-mail: lashajanelidze100@gmail.com

Reviewers:

M. Tabatadze, Associate Professor, Faculty of Informatics and Control Systems, GTU
E-mail: m.tabatadze@gtu.ge
N. Abzianidze, Associate Professor, Faculty of Informatics and Control Systems, GTU
E-mail: n.abzianidze@gtu.ge

Abstract. The rapid development of the digital era and the increasing demands of information technologies create a need to create more reliable, secure and efficient communication systems. In this context, quantum signals represent a technology of the future that responds to the challenges that classical signal systems can no longer cope with — for example, the highest level of information security, accuracy and transmission speed. The use of quantum entanglement, superposition and correlations makes it possible to protect and process information at the highest level. Accordingly, the implementation of quantum signals is critically important for areas such as quantum communication, secure cyberinfrastructure, high-tech sensors and quantum computing systems. The paper reviews the role of quantum signals in modern technologies and their potential in the near future. Quantum signal theory

combines the principles of quantum physics, information theory and signal processing. These features provide the highest accuracy in information transmission and processing, which is especially important in the development of quantum communication, quantum radars, and quantum sensors. This paper reviews the theoretical foundations of quantum signals, basic models, and their potential applications in modern technologies.

Keywords: BB84 protocol; Blox-Ben method; Cryptographic key; Photon; Polarization; Quantum entanglement; Quantum internet; Quantum mechanics; Quantum signal; Quantum state; Quantum superposition; Quantum teleportation; Quantum theory; Qubits.g

განხილვის თარიღი 04.07.2025
შემოსვლის თარიღი 08.07.2025
ხელმოწერილია დასაბეჭდად 24.12.2025