УДК 621.391

Н. В. Грабчак

ВИКОРИСТАННЯ КВАНТОВОЇ КРИПТОГРАФІЇ ДЛЯ ШИФРУВАННЯ ДАНИХ У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Вінницький національний технічний університет

Анотація

Сучасний світ увійшов в інформаційну епоху, де інфокомунікації визначають наше життя, спрощують спілкування, дозволяють доступ до безмежного обсягу знань та послуг. Ця доповідь присвячена вивченню сучасних проблем інфокомунікацій, які стають викликами для нашого суспільства. Ми розглянемо цифрову безпеку та кіберзагрози, приватність та обробку даних, доступ до інформації та інформаційну аналітику як основні аспекти цих проблем. Під час аналізу кожної проблеми, ми детально розглянемо її походження та причини, які спричинили її виникнення. Далі ми обговоримо можливі шляхи вирішення цих проблем, включаючи використання передових технологій та підходів.

Ключові слова: інформаційна аналітика, безпровідна мережа, цифрова безпека, приватність користувачів

Abstract

The modern world has entered the information age, where information and communication technologies define our lives, simplify communication, and provide access to an immense wealth of knowledge and services. This presentation is dedicated to the study of contemporary issues in infocommunications that pose challenges to our society. We will examine digital security and cyber threats, user privacy and data processing, access to information, and information analytics as the key aspects of these issues. When analyzing each problem, we will delve into its origins and the reasons that led to its emergence. Furthermore, we will discuss possible solutions to these problems, including the use of advanced technologies and approaches.

Keywords: information analytics, wireless network, digital security, user privacy

Вступ

Інфокомунікації – це не просто ключовий аспект сучасного світу, але і місто, яке живе в мережах безмежної інформації, де вся наша діяльність взаємопов'язана з обміном даними, комунікацією і доступом до величезних обсягів інформації. Це безумовно відкриває перед нами нескінченні можливості, але разом із тим створює значні виклики та проблеми. Тема "Сучасні проблеми інфокомунікацій" стає все більш актуальною, оскільки ми повинні зрозуміти ці виклики та працювати над їх вирішенням, щоб забезпечити стале функціонування нашого сучасного інформаційного суспільства.

На перший погляд, інфокомунікації здаються джерелом незмірних можливостей, що допомагають нам зв'язуватися зі світом, знаходити відповіді на питання та розвивати сучасну економіку. Проте ця інформаційна революція супроводжується новими викликами та загрозами, які ми повинні усунути для забезпечення стабільності та безпеки нашого суспільства.

З одного боку, ми спостерігаємо стрімке зростання кількості кіберзагроз та кібератак [2], що ставить під загрозу як наше цифрове майбутнє, так і власну безпеку. З іншого боку, збільшення обсягу зібраних особистих даних та їх неконтрольована обробка можуть порушувати нашу приватність та особисту свободу. Різниця в доступі до інформації може відокремлювати суспільство та залишати позаду певні групи населення. Окрім цього, зростання обсягів даних у цифровому світі вимагає нових методів інформаційної аналітики та обробки даних, аби зробити з них корисну інформацію

Метою роботи є дослідження викликів і проблем, які інфокомунікації приносять сучасному світові. Розвиток технологій та нові підходи в області інфокомунікацій можуть бути важливими інструментами в роботі над цими викликами. Основна мета - забезпечити безпечну, приватну та доступну інфокомунікаційну систему, яка сприятиме нашому соціальному та економічному розвитку.

Результати дослідження

З моменту появи інформаційних технологій сучасний світ дістався до інформаційної епохи, де інфокомунікації стали головною силою, що формує наше життя і спільність. Проте разом із безмежними можливостями, які надають інфокомунікації, приходять і складності. Однією з найзагостреніших проблем є цифрова безпека [2]. Взломи, кібератаки і зловживання даними стали частиною щоденної реальності. Потрібно розвивати прогресивні методи виявлення та запобігання атакам, використовувати системи раннього виявлення, інтелектуальний аналіз великих даних, і вдосконалювати технології шифрування і двофакторну аутентифікацію для забезпечення безпеки в інформаційному просторі.

Для вирішення цих проблем використовуються різні технології та підходи:

- Шифрування даних: Шифрування є ефективним способом захисту конфіденційної інформації. Важливо використовувати сучасні шифри та алгоритми шифрування для захисту даних в спокійному та транзитному стані. Ключовою технологією в цьому контексті є розвиток квантового шифрування [1].
- Анонімізація та псевдонімізація даних: Ці підходи дозволяють зберігати корисну інформацію в зашифрованому або анонімному вигляді, зберігаючи при цьому захист особистих даних. Для їх подальшого розвитку потрібно створити більш складні методи анонімізації та розробити ефективні методи перевірки якості анонімізації.
- Квантове шифрування: Квантова криптографія - це революційна технологія, яка використовує закони квантової механіки для забезпечення безпеки комунікацій [2]. Завдяки особливостям квантових бітів (кубітів), квантове шифрування дозволяє виявити будь-яку спробу підслуховування або зміни інформації. Коли квантові кубіти використовуються для обміну ключами, це забезпечує абсолютну безпеку даних. Проте ця технологія знаходиться на ранній стадії розвитку і потребує подальших досліджень та вдосконалення.

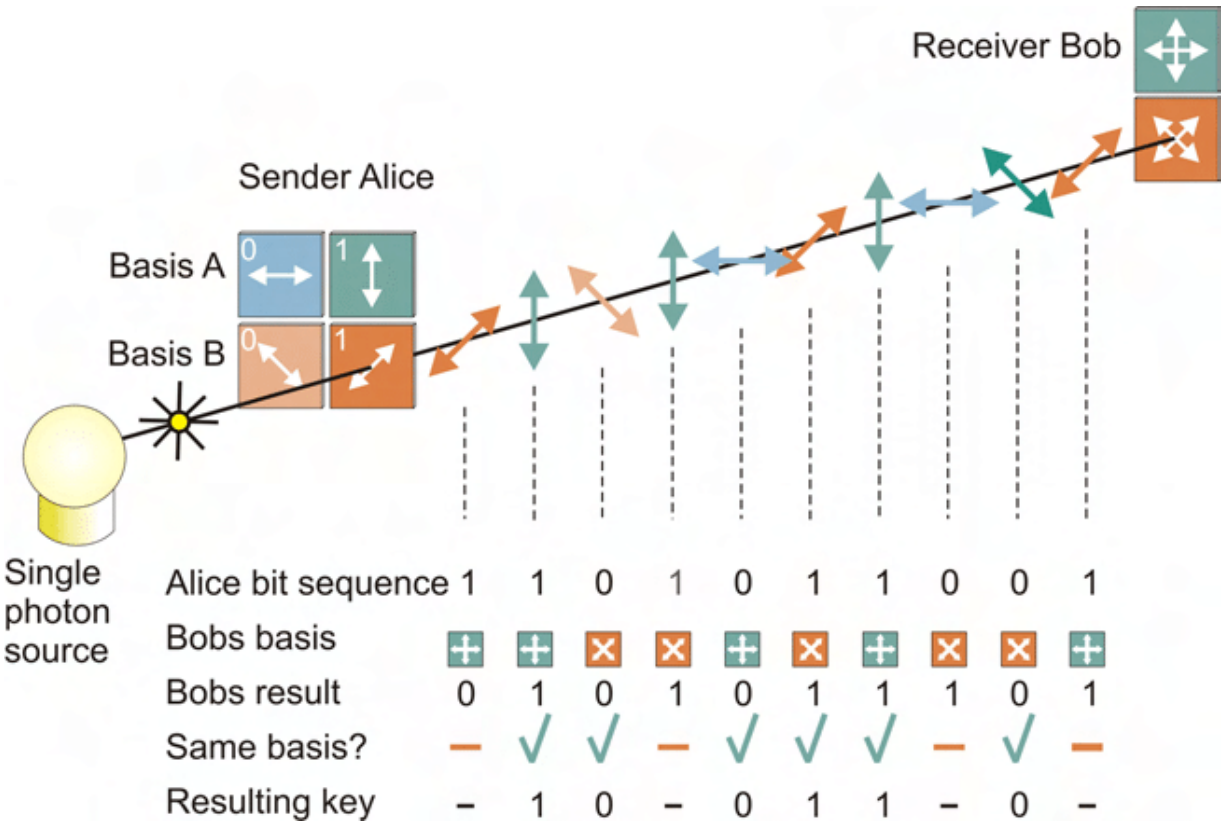

Рис. 1. Принцип роботи протоколу BB84 [1]. Аліса використовує два спряжених основи для кодування випадкової послідовності бітів. Лише біти, де Аліса та Боб використовували ту саму основу, беруться як ключ.

Для подальшого розвитку безпечних інформаційних технологій важливо інвестувати в дослідження квантової криптографії, яка може надати більшу стійкість до атак. Основні принципи квантової криптографії включають:

- Принцип несерйозного втручання (No-Cloning Principle): Згідно з цим принципом, неможливо створити точну копію квантового стану без зміни цього стану [1]. Це робить квантовий обмін даними вкрай стійким до підслуховування.
- Принцип невизначеності (Uncertainty Principle): Завдяки принципу невизначеності Гейзенберга, який стосується вимірювання квантових станів, важко визначити якість інформації, навіть якщо дані піддаються спробам перехоплення.
- Принцип квантового позначення (Quantum Entanglement): Цей принцип дозволяє створити пари квантових об'єктів, де стан одного об'єкта залежить від стану іншого, навіть при великій відстані [1]. Це робить неможливим перехоплення інформації без відома відправника і отримувача.

Квантове шифрування передбачає використання цих принципів для створення і обміну квантовими ключами. Квантові ключі використовуються для шифрування та дешифрування даних і гарантують безпеку комунікацій від підслуховування. Щоб покращити цю технологію, потрібно розвивати квантові комунікаційні пристрої, які були б більш стійкими до зовнішніх впливів [2], поліпшувати процеси виробництва квантових бітів та зменшувати їхню вартість, розробляти стандарти та протоколи квантового шифрування для їх придатності в реальних системах комунікацій.

Висновки

Розвиток квантової криптографії є ключовим для майбутнього цифрового світу і інфокомунікацій, оскільки вона надає найвищий рівень безпеки для обміну даними та дозволяє виявити будь-яку спробу підслуховування або зміни інформації. Квантова криптографія також стає ефективним засобом захисту від кіберзагроз, допомагаючи забезпечити безпеку в інформаційному просторі, де загрози стають все більшими і складнішими. Ця технологія відкриває нові можливості для розвитку квантового інтернету, де комунікації стають стійкими до будь-яких видів атак та змін, і може стати глобальним стандартом безпеки в інтернеті, забезпечуючи захист даних на всій планеті. Однак розвиток квантової криптографії потребує подальших досліджень, інновацій та інвестицій для поліпшення та комерціалізації квантових технологій, і вона стане невід'ємною частиною цифрового світу, забезпечуючи безпеку та конфіденційність наших даних у майбутньому.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. C. H. Bennet and G. Brassard, Quantum cryptography: Public key distribution and coin tossing BT, in IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (1984).
2. C. Gobby, Z. L. Yuan, and A. J. Shields, Unconditionally securequantum key distribution over 50 km of standard telecom fibre,ElectronicLetters 40 (25), 1603 (2004).

Грабчак Назарій Віталійович — аспірант групи 172-23а, факультет інформаційних електронних систем, Вінницький національний технічний університет, Вінниця, e-mail: nazarii.hrabchak@gmail.com

Науковий керівник: ***Барась Святослав Тадіонович*** – канд. техн. наук, професор кафедри телекомунікаційних систем та телебачення, Вінницький національний технічний університет, Вінниця, e-mail: barasst03@gmail.com.

Nazarii Vitaliyovych Hrabchak — postgraduate of 172-23a group, Faculty of Information Electronic Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: nazarii.hrabchak@gmail.com

Supervisor: ***Baras Sviatoslav Tadionovych*** - candidate. Sc., professor of telecommunications systems and television, Vinnytsia National Technical University, Vinnytsia, e-mail: barasst03@gmail.com.