КВАНТОВІ КРИПТОСИСТЕМИ

Таранова Д.В., *студентка*; СумДУ, гр. ФЕ-41

Криптографія вивчає методи шифрування інформації. Основна задача: передати інформацію між двома сторонами так, щоб перехопити її було неможливо. Існує недолік: з кожним повідомленням необхідно передавати великий секретний код. З точки зору класичної фізики не існує способу заборонити вимірювання сигналу без його збурення, тому інформацію завжди можливо перехопити. Квантова фізика дає можливість винайти фізичний канал, у якому неможливо вкрасти інформацію, не змінивши її.

В якості передавача секретного коду виступають стани елементарних частинок, наприклад, фотонів у лініях волоконно-оптичного зв'язку. З принципу невизначеності Гейзенберга випливає, що неможливо виміряти один параметр фотона, не змінивши інший. Отже, можливо зафіксувати спробу «підслуховування» каналу і навіть дізнатися, скільки інформації було втрачено. Це є перевагою квантової криптографії.

У роботі розглянуто, як саме відбувається реалізація квантових криптосистем. Розглянуті загальні принципи роботи, які характерні для всіх алгоритмів, детально вивчені протоколи BB84 і B92, оскільки саме вони є базовими.

Спроби створити на практиці квантові криптосистеми ведуться багатьма компаніями та університетами. Значні успіхи були отримані організаціями IBM, Gap-Optique, Mitsubishi, Toshiba Research Europe, MagiQ.

Основними недоліками, що заважають вже зараз застосовувати криптосистеми, є: низька швидкість передачі сигналу і неможливість його передачі на великі відстані; необхідність застосування складних компонентів, які важко сумістити зі стандартними технологіями.

Висновок: незважаючи на значний прогрес у квантовій криптографії за останні роки, існуючі системи є скоріше цікавими науковими експериментами, а не готовими для загального застосування рішеннями.

Керівник: Лисенко О.В., *завідувач кафедри*