УДК 681.3.06

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ПЕРЕДАВАНОЇ ІНФОРМАЦІЇ В КАНАЛІ ЗВ'ЯЗКУ

Кільдишев Віталій, Тіхонов Андрій

ОНАЗ ім. О.С. Попова

Анотація

В роботі розглядаються питання захисту каналів телекомунікаційного зв'язку від природних завад і штучних загроз, а також базові принципи захисту каналів зв'язку. Визначено деякі умови для побудови надійного алгоритму шифрування даних. Розглянуто залежність між фізичною швидкістю передачі символів та швидкістю передачі корисної інформації при збільшенні надмірності шифрування. Проаналізовано особливості передачі і шифрування даних у каналах з квантовими ефектами.

Abstract

This paper is focused on the issues of telecommunication channels protection from the natural influences and artificial threats, as well as basic principles of communication channels protection. Some conditions for constructing a reliable data encryption algorithm are defined. The dependence is considered between the physical rate of symbols transmission and the speed of the useful information transfer while increase of encryption redundancy. The features are analyzed of data transmission and encryption in channels with quantum effects.

Вступ

Захист каналів зв'язку займає важливе місце в загальній системі інформаційної безпеки. У даній роботі розглядається поняття «канал зв'язку» як телекомунікаційної підсистеми, утвореної двома цифровими приймачами, з'єднаними фізичної лінією зв'язку, на яку можуть впливати різного роду природні (ненавмисні) і штучні (навмисні) перешкоди, а також може мати місце пасивний та/або активний несанкціонований доступ. У каналі зв'язку існує безліч різних типів загроз, і в залежності від кожного з них розробляються специфічні методи боротьби з ними [1−4].

Принципи захисту інформації в каналі зв'язку

Основною одиницею прийому-передачі даних на канальному рівні є символи або блоки символів. Найпростішим символом передачі даних є біт. Сучасні телекомунікаційні системи використовують більші символи, що містять від 2 до 64 біт і більше. Головна мета боротьби з природними перешкодами в каналі зв'язку - це підвищення достовірності інформації що передається, тобто обмеження ймовірності прийому помилкового символу. Для цього застосовують т.зв. надлишкове кодування, при якому на передавальній стороні змістовні блоки символів відображаються в розширені блоки передачі, аналіз яких на приймальній стороні каналу дозволяє виявити або виправити помилки певних типів.

Для захисту інформації в каналі зв'язку від несанкціонованого доступу типу «прослуховування» використовують різні методи криптографії (шифрування даних): заміна (підстановка) символів, перестановка, аналітичні перетворення шифрованих даних та інші. Поширений метод шифрування - це заміна переданих символів на символи з того ж самого алфавіту, здійснювана по секретним таблицям шифрування. На основі цього методу можна побудувати алгоритм, який в принципі не піддається дешифруванню при відсутності таблиці шифрування. Для цього достатньо, щоб множина символів підстановки утворювала випадкову послідовність довжиною не менше переданого повідомлення (з однаковою ймовірністю всіх символів підстановки і незалежністю між будь-якою парою символів підстановки). Обмеження такого методу шифрування

обумовлені технічними можливостями створення, обміну та зберігання таблиць шифрування великих розмірів.

Підвищення швидкості передачі і зменшення енергії на одиницю інформації в оптичних каналах обумовлює появу квантових ефектів, пов'язаних з нечіткою ідентифікацією прийнятих символів. З точки зору детектора сигналу, один і той символ (наприклад, один біт), що генерується на передавальній стороні каналу, може перебувати в двох станах (нуль і одиниця). При цьому відносні частоти появи нулів і одиниць наближаються до можливостям їх появи. Однак при однаковій фізичній швидкості передавання символів, збільшення надмірності переданих блоків символів призводить до зниження кількості корисної інформації. При цьому зменшується ймовірність помилок; це, в свою чергу, дозволяє збільшити фізичну швидкість передачі. В результаті взаємного впливу цих факторів може бути досягнуто загальне підвищення ефективності передавання корисної інформації.

Властивості каналу зв'язку з квантовими ефектами визначаються матрицею ймовірностей $Pi,k = p(i,k)$, де i - значення переданого символу, j - значення прийнятого символу. Ця матриця є чутливою до змін фізичних властивостей каналу, наприклад, при несанкціонованому доступі до каналу матриця зміниться в тій чи іншій мірі. Дана матриця є унікальною характеристикою каналу зв'язку, яка може бути досліджена в метрологічному експерименті, а далі використана для детектування сигналів та виявлення несанкціонованого доступу. Квантові методи у криптографії поки що знаходяться у стадії активного розвитку. Однією з основних проблем у квантовій криптографії є підвищення швидкості передачі даних на великі відстані.

Висновки

В каналах зв’язку мають місце як природні, так і штучні перешкоди і впливи. Для боротьби з природними завадами використовують методи завадостійкого кодування з детектуванням та виправленням помилок. Боротьба зі штучними впливами здійснюється різними методами, зокрема шифруванням даних, а також застосуванням квантових принципів, чутливих до несанкціонованого доступу. Квантові методи у криптографії знаходяться у стадії активного розвитку. Однією з актуальних задач квантової криптографіє є збільшення швидкодії квантових каналів зв’язку.

Список використаних джерел:

1. Защита каналов связи. – Режим доступу : http://www.bezpeka.com/files/lib_ru/book-domarev03/ch_14.pdf.

2. Ємельянов С.О. Систематизація методів та засобів технічного захисту інформації в телефонних каналах та лініях зв'язку / С.О. Ємельянов // Сучасна спеціальна техніка. – 2011. – № 2 (25). – с. 128−132.

3. Гончарова Л.Л. Основи захисту інформації в телекомунікаційних та комп’ютерних мережах / Л.Л. Гончарова, А.Д. Возненко, О.І. Стасюк, Ю.О. Коваль. – 2013. – Режим доступу : .http://lib.detut.edu.ua/files/Nauk_trud_vukladahiv/Fakultet%20Infrastruktur_ruxomuy_sklad%20%E2%80%9D/Kafedra_tel_texn_avtomatuka/nauk_trud_voznenko.pdf.

4. Василіу Є.В. Методи підвищення криптографічної стійкості та збільшення інформаційної місткості протоколів квантової криптографії / Є.В. Василіу // Автореферат дисертації на здобуття наукового ступеня доктора технічних наук. – 2011.