

$p \rightarrow \frac{idh}{2p} \cdot \frac{d}{dx}$. Тогда приближенный спектр полученного дифференциального оператора определится по формуле

$$E_n = \hbar \left(n + \frac{1}{2} \right) + \frac{3}{2} a \hbar^2 \left(n^2 + n + \frac{1}{4} \right)$$

где $\hbar = \frac{h}{2p}$. Эта формула совпадает с результа-

том стандартной теории возмущений с точностью до последнего слагаемого во второй скобке. В частности, при $a = 0$ имеем известный случай гармонического осциллятора.

СПИСОК ЛИТЕРАТУРЫ

1. Найфэ А.Х. Методы возмущений. М.:МИР, 1976, 455с.
2. Де Брёйн Н.Г. Асимптотические методы в анализе. М.: ИИЛ, 1961, 247 с.
3. Давыдов А.С. Квантовая механика. М.: Физматгиз, 1963, 748с.

АНАЛИЗ ПРОТОКОЛОВ КВАНТОВОЙ КРИПТОГРАФИИ BB84 И B92

Хайров И.Е., Троцюк Е.В.

Квантовая криптография представляет собой одно из многообещающих и уже реализованных в практических приложениях направлений в рамках квантовой теории информации. Методами квантовой криптографии удается создавать абсолютно случайные секретные ключи между пользователями квантовой линии связи. Для достижения абсолютной случайности биты ключа необходимо передавать посредством отдельных фотонов, параметры которых, в соответствии с квантовой физикой, являются неопределенными. В начале 80-х годов подобную схему предложили Чарльз Беннет (Charles Bennett) из IBM и Жиль Браскар (Gilles Brassard) из Монреальского университета. Данный протокол получил название BB84. Несколько позже, в 1992 году, была модернизирована эта схема и на свет появился новый протокол, названный B92.

В работе проводится сравнительный анализ указанных двух протоколов квантовой криптографии. Для этих целей разработана программа для ЭВМ. Данная программа позволяет визуально наблюдать работу протоколов при наличии и отсутствии несанкционированного доступа (НСД). На рис. 1 представлены примеры работы протоколов BB84 и B92 при наличии НСД методом непосредственного съема и генерации.



Рисунок 1. Пример работы протоколов BB84 и B92 при наличии НСД

В качестве выходных данных программа рассчитывает вероятность правильного приема ключевой информации легальными пользователями и вероятность попадания этой информации (или ее части) злоумышленнику, осуществляющему НСД.

Из рис. 1 видно, что наличие анализатора агента вносит существенную неопределенность в результаты измерения поляризации фотонов получателем. Действительно, в случае протокола BB84 на приемном конце квантовой линии связи регистрируется фотон с типом поляризации, ортогональным переданному фотону. В случае же протокола B92, легальным получа-

телем возможна регистрация фотона с ненулевой вероятностью, хотя его анализатор ориентирован ортогонально поляризатору отправителя, что невозможно при отсутствии НСД.

Основным отличием протоколов BB84 и B92 является то, что даже при отсутствии в канале несанкционированного съема информации вероятность правильной регистрации типа поляризации фотонов (формирование ключевой последовательности бит) в протоколе B92 в два раза меньше чем в протоколе BB84.