

На правах рукописи

Трушечкин Антон Сергеевич

ИССЛЕДОВАНИЕ АСИМПТОТИЧЕСКИХ СВОЙСТВ НЕКОТОРЫХ  
КВАНТОВОМЕХАНИЧЕСКИХ МОДЕЛЕЙ В ОГРАНИЧЕННЫХ ОБЛАСТЯХ

01.01.03 — Математическая физика

АВТОРЕФЕРАТ

диссертации на соискание учёной степени  
кандидата физико-математических наук

Москва — 2009

Работа выполнена в Математическом институте им. В. А. Стеклова РАН.

Научный руководитель: член-корреспондент РАН, доктор физико-математических наук  
Волович И. В.

Официальные оппоненты: доктор физико-математических наук,  
профессор  
Доброхотов С. Ю.

доктор физико-математических наук,  
профессор  
Манько В. И.

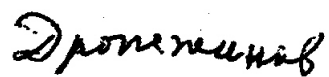
Ведущая организация: Механико-математический факультет Московского государственного университета им. М. В. Ломоносова

Защита состоится “ 17 ” декабря 2009 г. в 14 ч. 00 мин. на заседании Диссертационного совета Д 002.022.02 при Математическом институте им. В. А. Стеклова РАН по адресу: 119991, г. Москва, ул. Губкина, д. 8.

С диссертацией можно ознакомиться в научной библиотеке Математического института им. В. А. Стеклова РАН.

Автореферат разослан “ \_\_\_\_ ” ноября 2009 г.

Учёный секретарь Диссертационного совета  
доктор физико-математических наук

  
Ю. Н. Дрожжинов

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы.** Диссертационная работа посвящена исследованию асимптотических свойств некоторых квантовомеханических моделей в ограниченных областях. В настоящее время теория квантовомеханических систем в ограниченных областях является интенсивно развивающимся направлением. Это связано с тем, что квантовая механика в ограниченной области имеет существенные отличия от общеизвестной квантовой механики в неограниченной области, и вместе с тем аппарат квантовой механики в ограниченной области оказывается полезным в ряде случаев, например, при описании наноскопических систем, локализованных в соответствующих областях пространства.

В квантовой механике хорошо известны введённые Шрёдингером когерентные состояния (т.е. квадратично интегрируемые функции специального вида) на вещественной прямой. Поведение квантовой системы в состояниях, описываемых такими функциями, в определённом смысле близко к поведению соответствующих классических систем. Позже когерентные состояния рассматривались фон Нейманом. Само понятие «когерентные состояния» ввёл Р. Дж. Глаубер (R. J. Glauber), внёсший существенный вклад в метод когерентных состояний и получивший Нобелевскую премию в 2005 г. Метод когерентных состояний показал свою эффективность в изучении многих квантовых систем. В работах В. И. Манько, В. А. Малкина и А. М. Переломова показано, что когерентные состояния можно ввести для квантовой системы с использованием динамических симметрий и теории представлений групп. Метод когерентных состояний оказывается близким по духу методу интеграла по путям, введённому Фейнманом. Оба метода дают возможность проследить связь между классической и квантовой механикой и сделать наглядным квазиклассический предельный переход. Важный вклад в теорию квазиклассического предела внесли работы В. П. Маслова, С. Ю. Доброхотова, М. В. Карасёва, К. Хеппа (K. Hepp), а в теорию интеграла по путям — работы О. Г. Смолянова и Е. Т. Шавгулидзе. Обобщением когерентных состояний являются сжатые состояния, которые получаются из когерентных состояний при помощи операции сжатия.

Когерентные и сжатые состояния на многообразиях и в ограниченных

областях пространства для случаев, представляющих интерес для приложений, изучены значительно меньше, в текущей литературе продолжается обсуждение их определений и свойств. В частности, можно отметить математические работы по геометрическому квантованию и деформационному квантованию на многообразиях.

Заметим, что исследование таких состояний может оказаться полезным при рассмотрении наносистем. Важные исследования в этом направлении были выполнены В. П. Масловым, С. Ю. Доброхотовым, М. В. Карасёвым и другими. Для того чтобы можно было оперировать с наносистемами, требуется возможность достаточно точной локализации квантовых частиц в приемлемом диапазоне импульсов. Без дополнительного анализа неочевидно, что существуют квантовые состояния в ограниченном объёме, для которых возможна локализация квантовых частиц с точностью, необходимой для предполагаемых операций в нанотехнологиях.

Классическая динамика бесстолкновительной сплошной среды была исследована Пуанкаре и В. В. Козловым. Ими был установлен эффект диффузии для такой системы. Эволюция функции Вигнера и диффузия в бесстолкновительной среде, состоящей из квантовых частиц в некомпактном пространстве, были исследованы В. В. Козловым и О. Г. Смоляновым. Другой по сравнению с функцией Вигнера способ сопоставления квантовому оператору плотности классической функции плотности вероятностей на фазовом пространстве предложен К. Хусими (K. Husimi). Томографический вероятностный подход к описанию квантовомеханических систем был развит в работах В. И. Манько и соавторов.

Актуальной является также задача динамики квантовых волновых пакетов в ограниченных областях. Она изучалась в работах И. Ш. Авербуха, Н. Ф. Перельмана, Д. Л. Аронштейна (D. L. Aronstein), К. Р. Штрауда (мл.) (C. R. Stroud, Jr.), Р. В. Робинетта (R. W. Robinett). Однако некоторые вопросы остаются открытыми, например, математическое обоснование достижения квантовым волновым пакетом координатного распределения, близкого к равномерному.

Также в диссертации затрагивается известная проблема необратимости. Она заключается в том, как согласовать обратимую микроскопическую

динамику с необратимой макроскопической динамикой. Эта проблема впервые была осознана Больцманом, обсуждалась затем в известных работах Пуанкаре, фон Неймана, Боголюбова, Ландау, Пригожина, В. В. Козлова и многих других авторов. Проблема необратимости является в настоящее время одной из важнейших фундаментальных проблем математической физики, требующих своего решения.

Ещё один класс примеров квантовомеханических систем в ограниченных областях образуют системы квантовой криптографии. Квантовая криптография берёт начало от работы Ч. Беннетта (С. Н. Bennett) и Дж. Brassara (G. Brassard) и предлагает использовать специфические особенности квантовых частиц для защиты информации. Важный вклад в теорию квантовых каналов связи внёс А. С. Холево. В настоящее время квантовая криптография является интенсивно развивающимся направлением, уже существуют коммерческие системы квантового распределения ключей. Однако отсутствует математически строгая достаточно общая модель квантового распределения ключей. Важной задачей является создание такой модели, математическое обоснование стойкости протоколов квантовой криптографии, а также задача выработки числовых характеристик этой стойкости, которые должны указывать производители коммерческих систем квантовой криптографии.

С точки зрения пространства–времени системы квантовой криптографии являются квантовыми системами в ограниченных областях, необходимость учёта пространственной зависимости в квантовых криптографических системах при расчёте их стойкости указана И. В. Воловичем.

**Цель работы.** Целью работы является исследование асимптотических свойств квантовых когерентных и сжатых состояний в ограниченной области. А именно, исследование свойств локализации этих состояний по координате и по импульсу (т.е. статических свойств) и исследование квазиклассического предела их динамики.

Другой целью работы является разработка общей математической модели квантового распределения ключей и доказательство стойкости для некоторой частной модели.

**Научная новизна.** Все результаты диссертации являются новыми. Ос-

новные из них состоят в следующем:

- 1) Построены квантовые когерентные состояния для частицы в бесконечно глубокой потенциальной яме, доказана теорема об их квазиклассическом поведении на всех масштабах времени, что позволяет подробно проследить все этапы квантовой динамики. В частности, получено математическое обоснование асимптотического выравнивания плотности вероятности в конечном объёме для квантового случая, известного ранее лишь из численных расчётов;
- 2) Построены семейства квантовых сжатых состояний на отрезке, исследованы их асимптотические свойства локализации. Получены оценки дисперсии координаты и импульса для квантовой частицы на отрезке, применимые, в частности, для наноскопических систем;
- 3) Разработана общая математическая модель квантового распределения ключей, основанная на концепциях машины Тьюринга и квантового канала. Построена частная модель квантового распределения ключей, являющаяся аналогом известной классической модели, и доказана теорема о её стойкости. Рассмотрена проблема спецификации систем квантового распределения ключей: введена базовая функциональная характеристика — среднее время генерации ключей — и другие функциональные и числовые характеристики таких систем.

**Методы исследования.** В диссертации используются методы функционального анализа, теории операторов, теории обобщённых функций, асимптотические методы, методы квантовой теории информации.

**Теоретическая и практическая ценность.** Настоящая работа носит теоретический характер. Результаты, полученные в главе 1, могут использоваться для расчёта свойств локализации в наноскопических системах. Результаты, полученные в главе 2, могут быть использованы для анализа динамики квантовых волновых пакетов на окружности и в бесконечно глубокой потенциальной яме. Результаты, полученные в главе 3, могут быть использованы для анализа стойкости некоторых систем квантового распределения ключей, также в этой главе предлагается список функциональных и

числовых характеристик, которые должны указывать производители таких систем.

**Апробация работы.** Результаты работы докладывались автором на следующих международных конференциях: “5th Mathematical Physics Meeting: Summer School and Conference on Modern Mathematical Physics”, Белград (Сербия), 2008 г., «Международная конференция по математической физике и её приложениям», Самара, 2008 г., “International Bogolyubov Conference: Problems of Theoretical and Mathematical Physics” — международная конференция, посвящённая 100-летию со дня рождения Н. Н. Боголюбова, Москва—Дубна, 2009 г., на семинарах отдела математической физики Математического института им. В. А. Стеклова РАН, спецсеминаре «Математические вопросы динамики классических и квантовых систем», действующего в рамках Научно-образовательного центра при МИАН, на семинаре на Механико-математическом факультете МГУ под руководством О. Г. Смолянова.

**Публикации.** Основные результаты, перечисленные выше, опубликованы в работах [1—6].

**Структура и объём работы.** Диссертация состоит из введения, трёх глав, заключения, приложений и библиографии. Объём диссертации составляет 156 страниц. Библиография включает 88 наименований.

## ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность исследуемой проблемы, приводится краткий исторический обзор по теме диссертации, кратко излагаются основные результаты, а также описывается структура диссертационной работы.

В начале **главы 1** приводится описание модели квантовой частицы на отрезке. Затем разными способами конструируются сжатые состояния на отрезке и доказываются теоремы об их асимптотических локализационных свойствах. Квантовой частицей на отрезке  $[-l, l]$  будем называть произвольную квантовую систему, которой соответствует гильбертово пространство  $L_2(-l, l)$  — пространство комплекснозначных функций, определённых на отрезке  $[-l, l]$ , с интегрируемым квадратом модуля.

Под квантовым состоянием мы понимаем произвольный единичный вектор в рассматриваемом гильбертовом пространстве. Если  $v$  — вектор, не являющийся единичным, то под выражением «состояние  $v$ » будем понимать состояние  $\frac{v}{\|v\|}$ . Также в этой работе мы будем употреблять термин «квантовый волновой пакет» как синоним квантового состояния. Как правило, в данной работе подразумевается, что волновой пакет должен быть хорошо локализован, т.е. иметь малые дисперсии координаты и импульса.

Для квантовой частицы на прямой (т.е. для квантовой системы, которой соответствует гильбертово пространство  $L_2(\mathbb{R})$ ) хорошо известны соотношения неопределённостей Гейзенберга  $\Delta x \Delta p \geq \frac{\hbar}{2}$  и состояния, минимизирующие эти соотношения (т.е. для которых выполнено  $\Delta x \Delta p = \frac{\hbar}{2}$ ):

$$\eta_{qp}(x) = \frac{1}{\sqrt[4]{2\pi\alpha^2}} e^{-\frac{(x-q)^2}{4\alpha^2} + \frac{ip(x-q)}{\hbar}}.$$

Эти состояния называются сжатыми (или когерентными, если зафиксирован параметр  $\alpha > 0$ ).

Но для квантовой частицы на отрезке соотношения неопределённостей в обычном виде, вообще говоря, неверны. Например, для состояния  $\psi = \frac{1}{\sqrt{2l}} e^{i\frac{\pi}{l} kx}$  выполнено  $\Delta x = \frac{l}{\sqrt{3}}$  (вообще,  $\Delta x$  в конечном объёме не может быть бесконечным) и  $\Delta p = 0$  (импульс в данном состоянии хорошо определён и равен  $p_k = \frac{\pi}{l} \hbar k$ ). Отсюда имеем  $\Delta x \Delta p = 0$ .

Тем не менее, квантовая дополнительность между координатой и импульсом для квантовой частицы на отрезке также имеет место. Вопрос о том, как должны выглядеть соотношения неопределённостей для ограниченных областей, остаётся открытым и в настоящее время интенсивно обсуждается.

Наша задача состоит в том, чтобы построить аналог сжатых состояний (т.е. состояний, наиболее хорошо локализованных одновременно по координате и по импульсу) для отрезка. Поскольку нет общепринятого вида соотношений неопределённостей в ограниченной области, то за основу определения сжатых состояний на отрезке мы взяли условие асимптотической минимизации обычных соотношений неопределённостей на прямой.



Рассмотрим следующее семейство векторов из  $L_2(-l, l)$ :

$$\psi_\alpha(x) = \frac{1}{\sqrt{2l}} \sum_{k=-\infty}^{+\infty} a_k^{(\alpha)} e^{i\frac{\pi}{l}k(x-x^*)},$$

где  $a_k^{(\alpha)} = A_\alpha e^{-\frac{(k-k^*)^2}{4\alpha^2}}$ ,  $\alpha > 0$  — параметр семейства (как мы увидим, он связан со среднеквадратичным отклонением координаты),  $A_\alpha$  — нормировочная постоянная, такая, что  $\|\psi_\alpha\| = 1$ ,  $x^* \in (-l, l)$  (имеет смысл заданного значения координаты),  $k^*$  — ближайшее целое к  $\frac{l}{\pi} \frac{p^*}{\hbar}$ , где  $p^* \in \mathbb{R}$  (имеет смысл заданного значения импульса),  $\hbar > 0$  — постоянная Планка.

Функции  $\psi_\alpha$  могут быть выражены также следующим образом:

$$\psi_\alpha(x) = \frac{A_\alpha}{\sqrt{2l}} \theta\left(\frac{x-x^*}{2l}, \frac{1}{4\pi\alpha^2}\right) e^{i\frac{\pi}{l}k^*(x-x^*)},$$

где

$$\theta(x, \tau) = \sum_{k=-\infty}^{+\infty} e^{-\pi\tau k^2 + 2\pi i k x}$$

— тета-функция ( $\text{Re } \tau > 0$ ).

Определим следующие величины:

$$\bar{x}_\alpha = \int_{-l}^l x |\psi_\alpha(x)|^2 dx, \quad \bar{p}_\alpha = \sum_{k=-\infty}^{+\infty} p_k |a_k^{(\alpha)}|^2$$

(средние значения координаты и импульса), где  $p_k = \frac{\pi}{l} \hbar k$ ,

$$\Delta_* x_\alpha^2 = \int_{-l}^l (x-x^*)^2 |\psi(x)|^2 dx, \quad \Delta_* p_\alpha^2 = \sum_{k=-\infty}^{+\infty} (p_k - p^*)^2 |a_k|^2$$

(вторые моменты координаты и импульса, являются дисперсиями  $\Delta x_\alpha$  и  $\Delta p_\alpha$ , если  $x^* = \bar{x}$  и  $p^* = \bar{p}$ , но в общем случае эти равенства не выполнены).

Справедлива следующая

**Теорема 1.** Для волновых функций  $\psi_\alpha(x)$ ,  $\alpha > 0$ , справедливы следующие

оценки при  $\alpha \rightarrow \infty$ :

$$\begin{aligned}\psi_\alpha(x) &= \sqrt[4]{\frac{2\pi\alpha^2}{l^2}} e^{-(\alpha\pi d(\frac{x-x^*}{l}))^2 + i\frac{\pi}{l}k^*(x-x^*)} + O(\sqrt{\alpha}e^{-(\pi\alpha)^2}), \\ \bar{x}_\alpha - x^* &= l O\left(\alpha^{-1}e^{-2[\pi\alpha(1-\frac{|x^*|}{l})]^2}\right), \quad |\bar{p}_\alpha - p^*| \leq \frac{\pi}{l}\hbar, \\ \Delta_*x_\alpha^2 &= \left(\frac{l}{2\pi\alpha}\right)^2 + l^2 O\left(\alpha^{-1}e^{-2[\pi\alpha(1-\frac{|x^*|}{l})]^2}\right), \\ \Delta_*p_\alpha^2 &= \left(\frac{\pi}{l}\hbar\alpha\right)^2 [1 + O(e^{-2(\pi\alpha)^2})].\end{aligned}$$

Здесь  $0 \leq d(x) \leq \frac{1}{2}$  — расстояние на вещественной прямой от точки  $x$  до ближайшего целого числа.

Благодаря некоторым свойствам, в частности, свойству асимптотической минимизации соотношений неопределённостей

$$\lim_{\alpha \rightarrow \infty} \Delta x_\alpha \Delta p_\alpha = \frac{\hbar}{2},$$

построенное семейство  $\psi_\alpha$ ,  $\alpha > 0$ , векторов из  $L_2(-l, l)$  мы называем *квантовыми сжатыми состояниями на отрезке*.

Также в главе 1 доказана теорема об оценках на величины  $\bar{x}_\alpha$ ,  $\bar{p}_\alpha$ ,  $\Delta_*x$  и  $\Delta_*p$  для общего случая, когда коэффициенты Фурье  $a_k^{(\alpha)}$  функций семейства  $\psi_\alpha$ ,  $\alpha > 0$ , строятся на основе непрерывного распределения общего вида. Осуществляется предел  $l \rightarrow \infty$  и квазиклассический предел.

В главе 2 изучаются некоторые вопросы динамики когерентных состояний на окружности и в ящике (бесконечно глубокой потенциальной яме с твёрдыми стенками). Приведём здесь результаты для случая ящика. Определим следующее семейство состояний в  $L_2(-l, l)$ :

$$\omega_{qp}(x) = \sum_{n=-\infty}^{+\infty} (-1)^n \eta_{qp} [(-1)^n (x - 2nl)],$$

где  $(q, p) \in \Omega = [-l, l] \times \mathbb{R}$ . Справедлива следующая

**Теорема 2.** Семейство функций  $\omega_{qp}$ ,  $(q, p) \in \Omega$ , образует непрерывное разложение единицы в  $L_2(-l, l)$ :

$$\frac{1}{2\pi\hbar} \iint_{\Omega} P[\omega_{qp}] dq dp = 1.$$

Равенство понимается в слабом смысле: для любых  $\varphi, \varkappa \in L_2(-l, l)$  выполнено

$$\frac{1}{2\pi\hbar} \iint_{\Omega} (\varphi, P[\omega_{qp}]\varkappa) dqdp = \frac{1}{2\pi\hbar} \iint_{\Omega} (\varphi, \omega_{qp})(\omega_{qp}, \varkappa) dqdp = (\varphi, \varkappa).$$

Здесь через  $P[\psi]$ ,  $\psi \in L_2(-l, l)$ , обозначен одномерный оператор, действующий на произвольный вектор  $\varphi \in L_2(-l, l)$  по правилу  $P[\psi]\varphi = (\psi, \varphi)\psi$ , где  $(\cdot, \cdot)$  — скалярное произведение в  $L_2(-l, l)$ .

Эта теорема позволяет назвать векторы  $\omega_{qp}$  когерентными состояниями в  $L_2(-l, l)$ , если следовать определению Дж. Клаудера (J. R. Klauder) и Б.-С. Скагерштама (B.-S. Skagerstam). Оказывается, каждый вектор из этого семейства раскладывается в равномерно сходящийся ряд по собственным функциям оператора Гамильтона для ящика, поэтому назовём их *когерентными состояниями в ящике (в бесконечно глубокой потенциальной яме)*. Они родственны сжатым состояниям, введённым в главе 1, и также могут быть выражены через тета-функцию.

Эволюция состояния  $\omega_{qp}$  во времени даётся формулой  $\omega_{qp,t} = U_t^b \omega_{qp}$ , где  $U_t^b = \exp(-\frac{it}{\hbar} H^b)$  — оператор эволюции для свободной квантовой частицы в ящике. В его определении участвует оператор Гамильтона (энергии)  $H^b = -\frac{\hbar^2}{2m} \frac{d^2}{dx^2}$ ,  $m > 0$  (масса частицы), с областью определения  $D(H^b) = \{\psi \in AC^2(-l, l) \mid \psi(-l) = \psi(l) = 0\}$ . Здесь  $AC^2(-l, l)$  — множество дифференцируемых функций, чьи производные лежат в  $AC(-l, l)$ , а  $AC(-l, l)$  — множество абсолютно непрерывных функций, чьи производные лежат в  $L_2(-l, l)$ .

Для квантовой динамики в ящике имеют место три масштаба времени: 1)  $T_{cl} = \frac{4lm}{p}$  — классический период движения, 2)  $T_{coll} = \frac{16ml^2}{\pi\hbar}$  — характерное время расплывания квантового волнового пакета, 3)  $T_{rev} = \frac{16ml^2}{\pi\hbar}$  — период полного возрождения квантового волнового пакета (явление, характерное для квантовых систем в ограниченных областях).

Мы будем рассматривать квазиклассический предел  $\hbar \rightarrow 0$ ,  $\alpha \rightarrow 0$ ,  $\frac{\hbar}{\alpha} \rightarrow 0$  (параметр  $\alpha$  участвует в определении функций  $\omega_{qp}$ ). В этом пределе масштабы времени имеют разные асимптотики:  $T_{cl} = C_1$ ,  $T_{coll} = C_2 \frac{\alpha}{\hbar}$ ,  $T_{rev} = \frac{C_3}{\hbar}$  ( $C_1, C_2, C_3$  — постоянные).

Для того чтобы сформулировать основной результат по квазиклассическому пределу динамики этих состояний, определим пространства основных и обобщённых функций на полосе  $\Omega$ . Введём сначала пространство быстро убывающих функций на  $\Omega$ :

$$\begin{aligned} \mathcal{S}(\Omega) = \{ \sigma : \mathbb{R}^2 \rightarrow \mathbb{R} \mid & 1) \sigma[(-1)^n(q + 2nl), (-1)^n p] = \sigma(q, p); \\ & 2) \sigma \in C^\infty(\mathbb{R}^2); \\ & 3) \lim_{p \rightarrow \pm\infty} p^r \sigma^{(s)} = 0, r, s = 0, 1, 2, \dots \}. \end{aligned}$$

Здесь в первом пункте  $n = 0, \pm 1, \pm 2, \dots$ . Пространство обобщённых функций  $\mathcal{S}'(\Omega)$  – это пространство непрерывных линейных функционалов над  $\mathcal{S}(\Omega)$ . Если  $f(q, p) = f_1(q)\delta(p) \in \mathcal{S}'(\Omega)$ , где  $f_1(q)$  – интегрируемая функция на отрезке  $[-l, l]$ , то её действие на основную функцию  $\sigma \in \mathcal{S}(\Omega)$  определяется по формуле  $(f, \sigma) = \int_{-l}^l f_1(q)\sigma(q, 0)dq$ . Условимся считать, что  $(\delta(q - q_0, p - p_0), \sigma) = \sigma(q_0, p_0)$  при любых  $(q_0, p_0) \in \mathbb{R}^2$  (а не только при  $(q_0, p_0) \in \Omega$ ).

Определим функцию

$$\varphi_D(q) = \frac{1}{\sqrt{2\pi D^2}} \sum_{n=-\infty}^{+\infty} e^{-\frac{(q-4nl)^2}{2D^2}},$$

где  $D \in (0, \infty)$ . Доопределим функцию при  $D = 0$  и  $D = \infty$ :  $\varphi_0(q) = \delta(q)$  и  $\varphi_\infty(q) = \frac{1}{4l}$ . Таким образом, как обобщённая функция  $\varphi_D(q)$  определена при произвольном  $D \in [0, \infty]$ .

Справедлива следующая

**Теорема 3.** *В  $\mathcal{S}'(\Omega)$  имеют место следующие пределы (в обоих пунктах переменные  $(q, p)$  фиксированы, а  $(q', p')$  – переменные интегрирования с пробными функциями  $\sigma(q', p') \in \mathcal{S}(\Omega)$ ):*

$$\begin{aligned} & 1) \\ & \lim \left\{ \frac{1}{2\pi\hbar} |(\omega_{qp}, \omega_{q'p', t})|^2 - \right. \\ & \quad - \frac{1}{N'} \sum_{k=0}^{N'-1} \varphi_D \left[ q' - q - \frac{4kl}{N'} - a + \frac{p}{m} \left( t - \frac{M}{N} T_{rev} \right) \right] \delta(p' - p) - \\ & \quad \left. - \frac{1}{N'} \sum_{k=0}^{N'-1} \varphi_D \left[ q' - 2l + q + \frac{4kl}{N'} + a - \frac{p}{m} \left( t - \frac{M}{N} T_{rev} \right) \right] \delta(p' + p) \right\} = 0. \end{aligned} \quad (1)$$

Предел осуществляется следующим образом:  $\hbar \rightarrow 0$ ,  $\alpha \rightarrow 0$ ,  $\frac{\hbar}{\alpha} \rightarrow 0$ ,  $t = t(\hbar)$ ,  $\frac{\hbar}{\alpha}(t - \frac{M}{N}T_{rev}) \rightarrow 2mD$ , где  $M$  и  $N$  — взаимно простые целые числа (т.е.  $c = \frac{M}{N}$  — несократимая дробь),  $D \in [0, \infty]$ . Здесь  $N' = N$ , если  $N$  нечётно, и  $N' = \frac{N}{2}$  если  $N$  чётно;  $a = \frac{2l}{N}$ , если  $N = 2 \pmod{4}$ , и  $a = 0$  в противном случае;

2)

$$\lim \frac{1}{2\pi\hbar} |(\omega_{qp}, \omega_{q'p',t})|^2 = \frac{1}{4l} [\delta(p' - p) + \delta(p' + p)]. \quad (2)$$

Предел осуществляется следующим образом:  $\hbar \rightarrow 0$ ,  $\alpha \rightarrow 0$ ,  $\frac{\hbar}{\alpha} \rightarrow 0$ ,  $t \rightarrow \infty$ ,  $\hbar(t - cT_{rev}) \rightarrow 0$ , где  $c$  — иррациональное число.

Обе сходимости являются равномерными по  $(q, p)$  на любом подмножестве  $\Omega$ , не пересекающемся с некоторой окрестностью отрезка  $\{p = 0\} \subset \Omega$ . Если в первом пункте  $N = 1$  или  $N = 2$  (т.е.  $c = \frac{M}{N}$  — целое или полуцелое число), то сходимость является равномерной на любом подмножестве  $\Omega$ , не пересекающемся с некоторыми окрестностями точек  $(\pm l, 0)$ .

Поясним смысл утверждений теоремы.  $\frac{1}{2\pi\hbar} |(\omega_{qp}, \omega_{q'p',t})|^2$  представляет собой плотность вероятности нахождения квантовой частицы в ящике в состоянии  $\omega_{qp}$  в момент времени  $t$  при условии, что в нулевой момент времени частица находилась в состоянии  $\omega_{q'p'}$ .

В рассматриваемом квазиклассическом пределе  $\hbar, \alpha, \frac{\hbar}{\alpha} \rightarrow 0$  у квантовой частицы в состоянии  $\omega_{qp}$  хорошо определены и координата (равная  $q$ ), и импульс (равный  $p$ ) — как у классической частицы. Поэтому можно сказать, что в квазиклассическом пределе  $\frac{1}{2\pi\hbar} |(\omega_{qp}, \omega_{q'p',t})|^2$  — это плотность вероятности нахождения квантовой частицы в ящике в фазовой точке  $(q, p)$  в момент времени  $t$  при условии, что в нулевой момент времени частица находилась в фазовой точке  $(q', p')$ .

Случай  $c = 0$  и  $D = 0$  ( $\frac{\hbar t}{\alpha} \rightarrow 0$ ) соответствует первому, классическому, масштабу времени  $T_{cl}$ : время фиксировано или возрастает медленнее, чем снижается скорость расплывания пакета, пропорциональная  $\frac{\hbar}{\alpha}$ . Тогда формула (1) принимает вид

$$\lim \left[ \frac{1}{2\pi\hbar} |(\omega_{qp}, \omega_{q'p',t})|^2 - \delta(q' - q + \frac{p}{m}t, p' - p) \right] = 0.$$

Вычитаемое  $\delta(q' - q + \frac{p}{m}t, p' - p)$  правой части равенства есть плотность вероятности нахождения классической частицы в фазовой точке  $(q, p)$  в момент времени  $t$  при условии, что в нулевой момент времени частица находилась в фазовой точке  $(q', p')$ . Таким образом, в квазиклассическом пределе на масштабе времени  $T_{cl}$  имеет место классическая динамика: квантовая плотность вероятности перехода в фазовую точку  $(q, p)$  для частицы, находившейся в нулевой момент времени в фазовой точке  $(q', p')$ , равна соответствующей классической плотности вероятности.

Случай  $c = 0$ ,  $D \in (0, \infty)$  (т.е.  $\frac{\hbar t}{\alpha} \rightarrow 2mD$ ) соответствует второму масштабу времени  $T_{coll}$ . В этом случае наблюдается некоторое пространственное расплывание распределения вероятностей. Случай  $c = 0$ ,  $D = \infty$  соответствует полному выравниванию пространственной плотности вероятности (и вероятностей знаков импульса): формула (1) принимает вид

$$\lim \frac{1}{2\pi\hbar} |(\omega_{qp}, \omega_{q'p',t})|^2 = \frac{1}{4l} [\delta(p' - p) + \delta(p' + p)]. \quad (3)$$

Поэтому отнесём этот случай также ко второму масштабу времени (соответствующему разрушению локализованного волнового пакета). Получено математическое обоснование (асимптотического) выравнивания пространственной плотности вероятности для квантовой частицы в ящике, известное ранее лишь из численных экспериментов.

Случай  $c \neq 0$  соответствует третьему масштабу времени  $T_{rev}$ . Если  $c$  — иррациональное число, то, как и в предыдущем случае, наблюдается полное выравнивание пространственной плотности вероятности (формула (2)). Случай рационального  $c$  соответствует возрождению волнового пакета, в общем случае — дробному (если  $N \neq 1$ , т.е.  $c = \frac{M}{N}$  — нецелое) и неточному (если  $D > 0$ ). В случае  $D = \infty$  мы снова получаем полное выравнивание пространственной плотности распределения (3).

Мы только что проследили всю динамику квантового волнового пакета в бесконечно глубокой потенциальной яме. Таким образом, теорема полностью описывает квазиклассический предел свободной квантовой динамики в бесконечно глубокой потенциальной яме на всех масштабах времени, которые параметризуются двумя параметрами  $c$  и  $D$ .

Далее эти результаты применяются к вопросу, связанному с класси-

ческой механикой, а именно, к вопросу, какую формулировку классической механики следует предпочесть: обычную (будем называть её «точечной») или функциональной. Исходное понятие механики в функциональной формулировке, предложенной И. В. Воловичем, — не материальная точка, а функция плотности распределения в фазовом пространстве. Новая формулировка классической механики позволяет по-новому взглянуть на известную проблему необратимости.

Доказана теорема, которая говорит о том, что функциональная формулировка классической механики (т.е. динамика интегрируемой функции плотности в ящике) дольше сохраняет свою справедливость с точки зрения квантовой механики, нежели точечная формулировка (т.е. динамика материальной точки в ящике). Следовательно, с этой точки зрения функциональная формулировка является более предпочтительной. В теореме использована техника квазиклассического предельного перехода для преобразования Хусими в ящике, в котором участвуют построенные и изученные когерентные состояния.

**Глава 3** посвящена квантовой криптографии. В ней разработана общая математическая модель квантового распределения ключей, основанная на концепциях машины Тьюринга и квантового канала. Построена частная модель квантового распределения ключей, являющаяся аналогом известной модели классической криптографии, и доказана теорема о её стойкости.

Рассматриваемая задача распределения ключей заключается в следующем. Отправитель  $A$  и получатель  $B$  (законные участники) желают, используя каналы связи, получить по ключу. Под ключом понимается реализация случайной величины со значениями в некотором конечном множестве  $\mathcal{X}$  либо сама эта случайная величина. Если ключи у  $A$  и  $B$  с большой вероятностью совпадают, а информация о ключах у противника  $E$  пренебрежимо мала, то задача распределения ключей считается решенной с некоторой степенью надёжности.

Введём обозначения:  $\mathcal{P}(\mathcal{X})$  — множество распределений вероятностей на произвольном конечном множестве  $\mathcal{X}$ ,  $\mathcal{S}(\mathcal{H})$  — множество операторов плотности на произвольном гильбертовом пространстве  $\mathcal{H}$ ,  $\mathcal{M}(\mathcal{H}; \mathcal{X})$  — множество (обобщённых) наблюдаемых на  $\mathcal{H}$

со значениями в конечном множестве  $\mathcal{X}$ , т.е. множество наборов положительных операторов  $\{M(x)\}_{x \in \mathcal{X}}$ , такое, что  $\sum_{x \in \mathcal{X}} M(x) = 1$ . Обозначим через  $\mathcal{B}^{\mathcal{A}} \circ \mathcal{M}(\mathcal{H}; \mathcal{A}) \subset \mathcal{M}(\mathcal{H}; \mathcal{B})$  класс наблюдаемых вида  $\{F(b) = \sum_{a \in f^{-1}(b)} M(a)\}_{b \in \mathcal{B}}$ , где  $\{M(a)\}_{a \in \mathcal{A}} \in \mathcal{M}(\mathcal{H}_B; \mathcal{A})$ , а  $f$  — элемент множества  $\mathcal{B}^{\mathcal{A}}$  функций из  $\mathcal{B}$  в  $\mathcal{A}$ . Назовём элементы этого класса факторизованными наблюдаемыми с последующей классической обработкой.  $\Theta^n : \mathcal{S}(\mathcal{H}_A^{\otimes n}) \rightarrow \mathcal{S}[(\mathcal{H}_B \otimes \mathcal{H}_E)^{\otimes n}]$ ,  $n = 1, 2, \dots$ , — это квантовый канал без памяти, соответствующий каналу  $\Theta$ .

Рассмотрим следующую совокупность объектов (назовём её системой квантового распределения ключей  $G$ ):

$$G = \left( \mathcal{K}, \mathcal{H}_A, \mathcal{H}_B, \mathcal{H}_E, \Theta, \{q^{(n)}\}_{n=1}^{\infty}, \{M_B^{(n)}\}_{n=1}^{\infty}, \{M_E^{(n)}\}_{n=1}^{\infty} \right).$$

Здесь  $\mathcal{K}$  — конечное множество (множество ключей),  $\mathcal{H}_A, \mathcal{H}_B, \mathcal{H}_E$  — гильбертовы пространства,  $\Theta : \mathcal{S}(\mathcal{H}_A) \rightarrow \mathcal{S}(\mathcal{H}_B \otimes \mathcal{H}_E)$  — квантовый канал, функции  $q^{(n)} : \mathcal{K} \rightarrow \mathcal{S}(\mathcal{H}_A^{\otimes n})$  задают каналы  $Q^{(n)} : \mathcal{P}(\mathcal{K}) \rightarrow \mathcal{S}(\mathcal{H}_A^{\otimes n})$ ,  $M_B^{(n)} \in \mathcal{M}(\mathcal{H}_B^{\otimes n}; \mathcal{K})$ ,  $M_E^{(n)} \in \mathcal{M}(\mathcal{H}_E^{\otimes n}; \mathcal{K})$ .

Для каждого  $n = 1, 2, \dots$  и  $M_E^{(n)} \in \mathcal{M}_E^{(n)}$  определим канал  $\Lambda_n = (M_B^{(n)} \otimes M_E^{(n)}) \circ \Theta^n \circ Q^{(n)}$  с входным алфавитом  $\mathcal{K}$  и выходным алфавитом  $\mathcal{K}^2$ .

Обозначим через  $K_A$  случайную величину, равномерно распределённую на  $\mathcal{K}$  (ключ). Обозначим через  $K_B$  и  $K_E$  случайные величины, принимающие значения на  $\mathcal{K}$  и связанные с  $K_A$  каналом  $\Lambda_n$  при некотором  $n$ , т.е.  $(K_B, K_E) = \Lambda_n(K_A)$ . Схематическое изображение процесса квантового распределения ключей приведено на рис. 1.

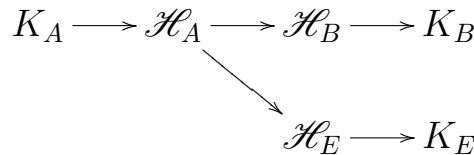


Рис. 1. Схема модели  $G$ .

Справедлива следующая теорема о стойкости системы  $G$  (через  $\text{Pr}(\cdot)$  обозначена вероятность события).

**Теорема 4.** В модели  $G$  квантового распределения ключей фиксируем  $\mathcal{H}_A$ ,



$\mathcal{H}_B, \mathcal{H}_E, \Theta$ . Для любого  $n = 1, 2, \dots$  положим  $\mathcal{M}_E^{(n)} = \mathcal{K}^{\mathcal{E}^n} \circ \mathcal{M}(\mathcal{H}_E; \mathcal{E})^{\otimes n}$ , где  $\mathcal{E}$  — конечное множество.

Пусть существуют конечное множество  $\mathcal{A}$  и канал  $\Xi : \mathcal{P}(\mathcal{A}) \rightarrow \mathcal{S}(\mathcal{H}_A)$ , задаваемый функцией  $\xi : \mathcal{A} \rightarrow \mathcal{S}(\mathcal{H}_A)$ , обладающие свойством

$$C(\Theta_B \circ \xi) > C_1(\Theta_E \circ \xi), \quad (4)$$

где  $\Theta_B = \text{Tr}_{\mathcal{H}_E} \Theta$ ,  $\Theta_E = \text{Tr}_{\mathcal{H}_B} \Theta$ ,  $C(\Theta_B \circ \xi)$  — пропускная способность канала  $\Theta_B \circ \Xi$ ,  $C_1(\Theta_E \circ \xi) = \max_{P \in \mathcal{P}(\mathcal{A}), M \in \mathcal{M}(\mathcal{H}_E; \mathcal{K})} I(P, M \circ \Theta_E \circ \Xi)$ .

Тогда для любых  $\alpha, \beta \in (0, 1)$  и любого достаточно большого  $n$  существуют канал (случайный кодер)  $F_A : \mathcal{P}(\mathcal{K}) \rightarrow \mathcal{P}(\mathcal{A}^n)$  и наблюдаемая  $M_B^{(n)} \in \mathcal{M}(\mathcal{H}_B^{\otimes n}; \mathcal{K})$ , такие, что для произвольной наблюдаемой  $M_E^{(n)} \in \mathcal{M}_E^{(n)}$  случайные величины  $K_A, K_B$  и  $K_E$ , где  $(K_B, K_E) = \Lambda_n(K_A)$ , обладают свойствами:

$$1) \Pr(K_A = K_B) \geq \alpha, \quad 2) I(K_A; K_E) \leq 1 - \beta.$$

Здесь  $Q^{(n)}$  в определении  $\Lambda_n$  равен  $Q^{(n)} = \Xi^n \circ F_A$ .

Величины  $\alpha$  и  $\beta$  характеризуют степень надёжности пары ключей законных участников и при выполнении условия (4) могут быть выбраны сколь угодно близкими к единице (совершенная надёжность). Таким образом, (4) является достаточным условием для того, чтобы система квантового распределения ключей  $G$  была стойкой к атакам противника. Более того, можно показать, что возможна ситуация идеального прослушивания квантового канала противником, в которой, тем не менее, возможно создание общего секретного ключа законными участниками. Эффект достигается за счёт использования отправителем неортогональных состояний для кодирования классической информации, а получателем — т.н. зацепленных наблюдаемых. Данному эффекту нет аналогов в классической криптографии, и в этом смысле можно говорить о преимуществах квантовой криптографии перед классической.

Также в третьей главе рассмотрена проблема спецификации систем квантового распределения ключей: введена базовая функциональная характеристика — среднее время генерации ключей — и другие функциональные и числовые характеристики таких систем.

## СПИСОК ПУБЛИКАЦИЙ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

1. Волович И. В., Трушечкин А. С. О квантовых сжатых состояниях на отрезке и соотношениях неопределённостей для наноскопических систем // Тр. МИАН. 2009. Т. 265. С. 288—319.
2. Волович И. В., Трушечкин А. С. Об одной проблеме распределения ключей в квантовой криптографии // ДАН. 2005. Т. 404, № 2. С. 169—172.
3. Трушечкин А. С. Квантовые когерентные состояния и соотношения неопределённостей для наноскопических систем // Вестник СамГУ. 2009. № 8/1(67). С. 254—273.
4. Trushechkin A. S., Volovich I. V. On standards and specifications in quantum cryptography // International Journal of Quantum Information. 2008. V. 6, N 2. P. 347—367.
5. Trushechkin A. S., Volovich I. V. Functional classical mechanics and rational numbers // P-Adic Numbers, Ultrametric Analysis and Applications. 2009. V. 1, N 4. P. 365—371.
6. Trushechkin A. S., Volovich I. V. Classical and quantum cryptography and number theory // AIP Conference Proceedings. V. 826. 2nd International conference on p-adic mathematical physics. New York : AIP, 2006. P. 345—354.