Моделирование релятивистской системы квантового распределения ключей

Дипломная работа

Большаков Роман Алексеевич
Научный руководитель: профессор,
д.ф-м.н. Молотков С.Н.

Московский государственный университет имени М.В. Ломоносова
Факультет вычислительной математики и кибернетики
Кафедра суперкомпьютеров и квантовой информатики

Москва, 2015

Квантовое распределение ключей — механизм:

- использующий фундаментальные принципы квантовой механики,
- в результате работы которого:
  - либо получается общая для двух участников коммуникации строка случайных бит, известная только им;
  - либо происходит детектирование злоумышленника в канале связи.

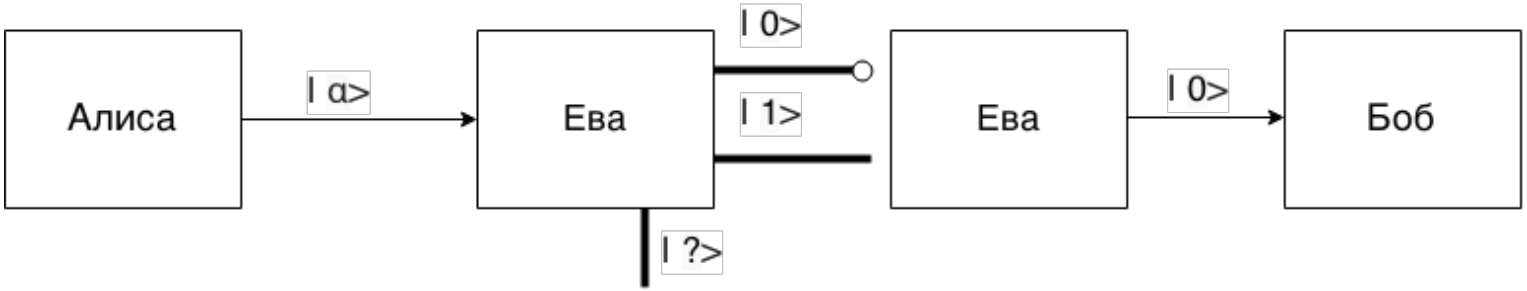
Проблемы практических реализаций

Основные практические проблемы имеющихся на данный момент протоколов:

- лазер испускает когерентное состояние:
  $|\alpha\rangle = e^{-\frac{\mu}{2}} \sum_{n=0}^{\infty} \frac{\sqrt{\mu}}{\sqrt{n!}} |n\rangle = e^{-\frac{\mu}{2}} (|0\rangle + \sqrt{\mu}|1\rangle + \frac{\mu}{\sqrt{2}}|2\rangle + \dots)$,
  где μ — среднее число фотонов в одном импульсе;
- потери в канале связи.

Атака на нерелятивистские протоколы

При указанных проблемах становится осуществима атака, основанная на измерениях с неопределенным исходом.



Если $Pr_{loss} > Pr_{?}$ — подслушиватель знает весь ключ и остается незамеченным.

Решение проблем

Нерелятивистские протоколы используют только ограничения квантовой механики.
Но:

- фотоны движутся со скоростью света (как все безмассовые частицы),
- а скорость света — предельно допустимая скорость распространения взаимодействий.

Квантовая механика $+$ СТО $=$ релятивистский протокол.

Цель дипломной работы

Целью данной дипломной работы является создание программных средств:

1. моделирования и визуализации релятивистского протокола квантового распределения ключей в открытом пространстве,
2. моделирования и визуализации каскадного протокола коррекции ошибок по аутентичному каналу.

Схема релятивистского протокола

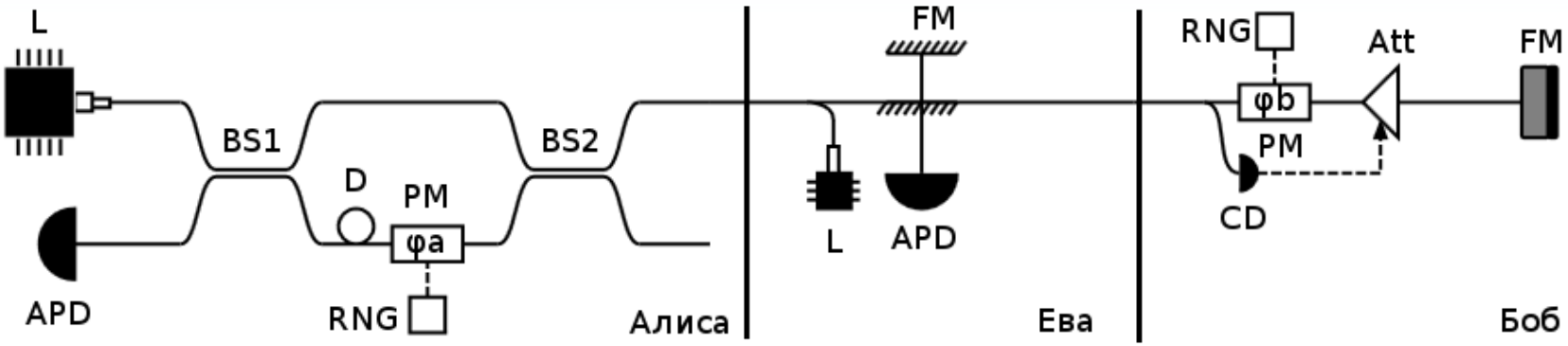


Схема релятивистского протокола

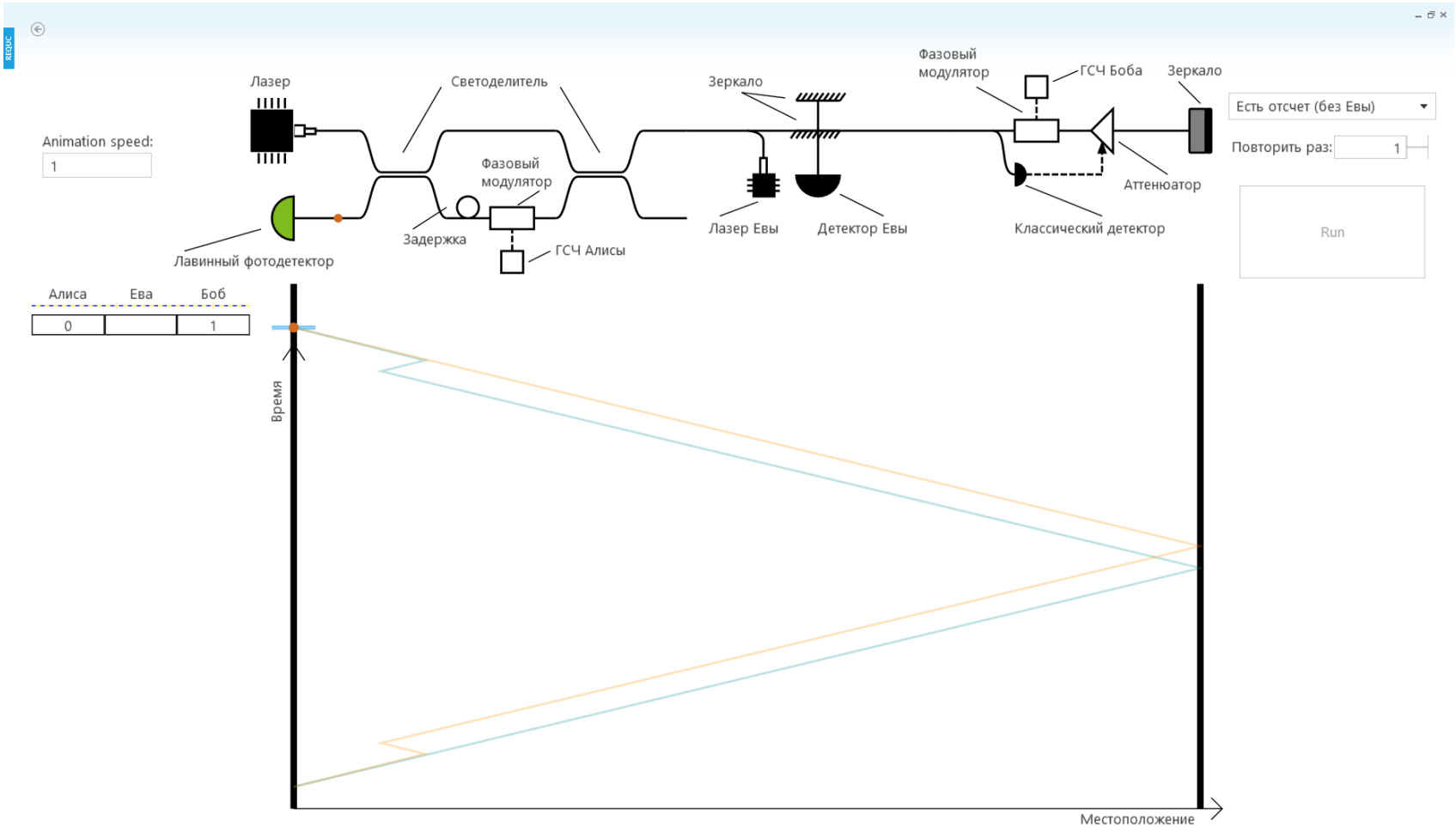


Схема релятивистского протокола

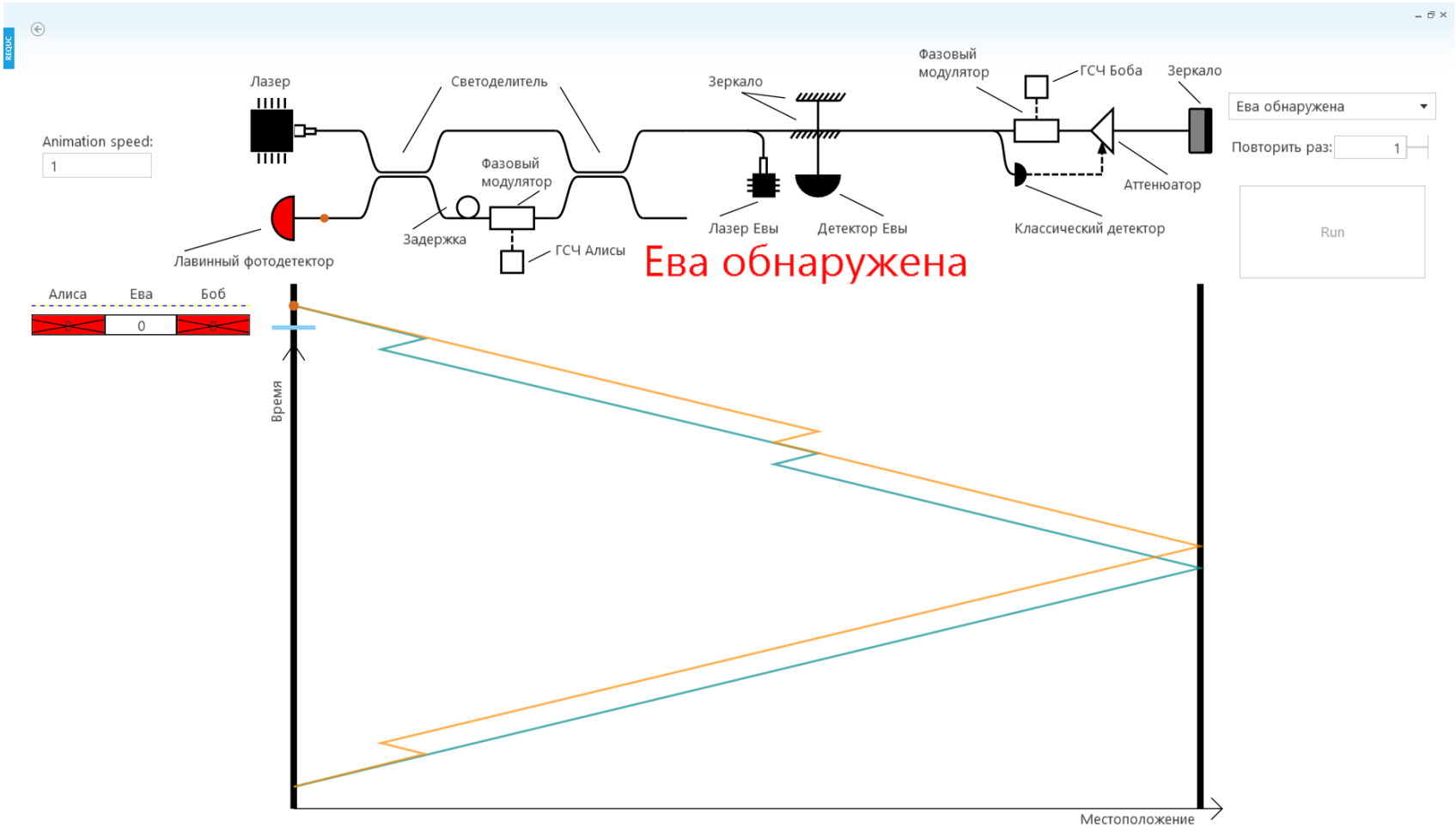
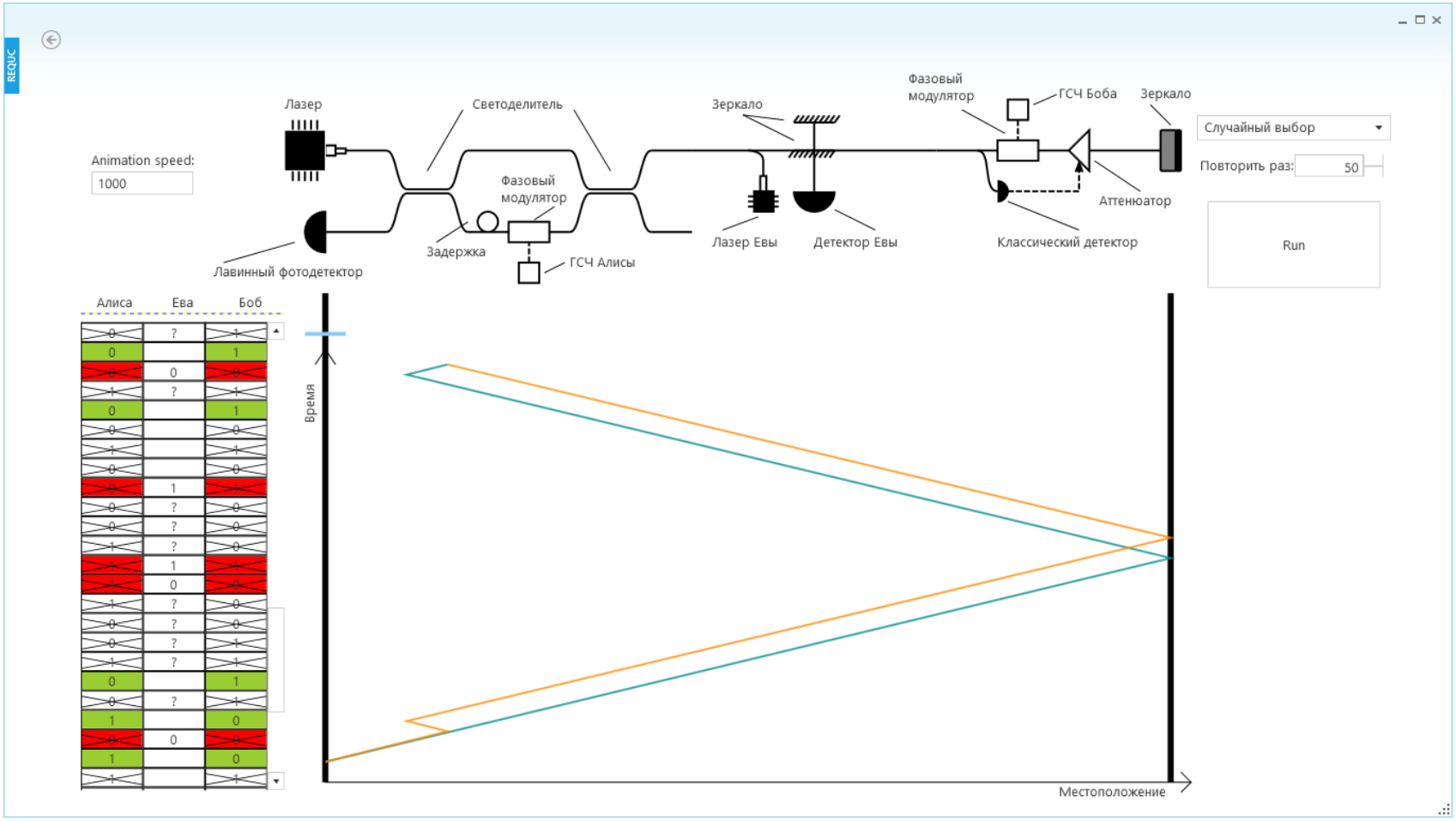


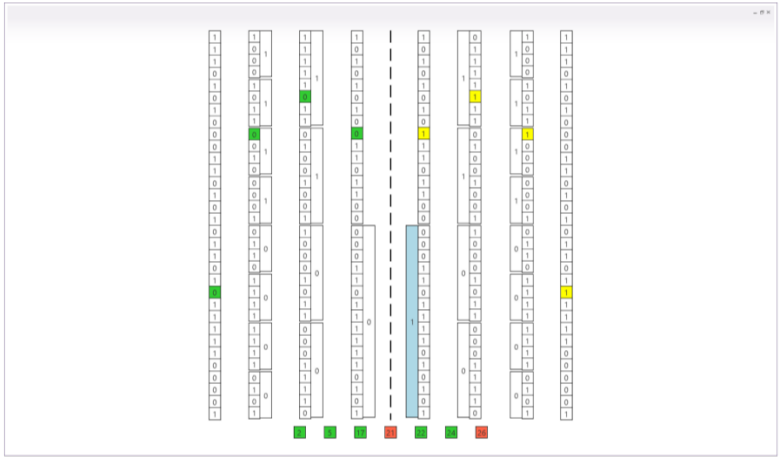
Схема релятивистского протокола

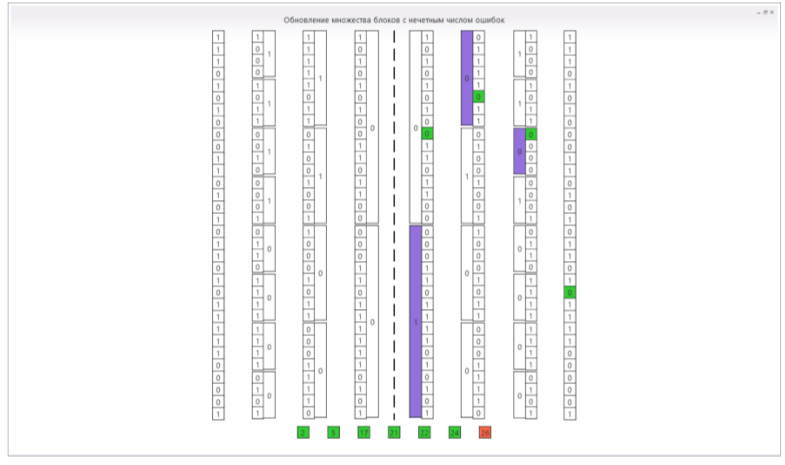


Каскадный метод коррекции ошибок

В канале связи (в частности если это открытое пространство) неизбежно присутствуют помехи, вносящие ошибки в ключ. Их необходимо исправить, выдав как можно меньше информации о ключе возможному подслушивателю.

Каскадный метод коррекции ошибок





Определение

Семейство $\mathcal{F}$ функций $\mathcal{A} \to \mathcal{B}$ называется *универсальным*, если

$$[f(x_1) = f(x_2)] < \frac{1}{|\mathcal{B}|} \quad \forall x_1, x_2 \in \mathcal{A} : x_1 \neq x_2,$$

а f выбирается из $\mathcal{F}$ в соответствии с равномерным распределением.

Полученные результаты

1. Проведен детальный анализ, моделирование и визуализация протокола квантовой криптографии, обеспечивающего безусловную секретность в условиях потерь в линии связи и неоднофотонности источника с обоснованием секретности.
2. Рассмотрен и смоделирован (в виде отдельной программы) один из протоколов коррекции ошибок, который в настоящее время является стандартом в квантовом распределении ключей.

Спасибо за внимание.

Моделирование релятивистской системы квантового распределения ключей

Дипломная работа

Большаков Роман Алексеевич
Научный руководитель: профессор,
д.ф-м.н. Молотков С.Н.

Московский государственный университет имени М.В. Ломоносова
Факультет вычислительной математики и кибернетики
Кафедра суперкомпьютеров и квантовой информатики

Москва, 2015