# ПЛАНИРОВАНИЕ ЭКСПЕРИМЕНТА И ПРОГРАММНЫЕ ПАКЕТЫ ДЛЯ АНАЛИЗА ИНФОРМАТИВНОСТИ И ИНТЕРПРЕТАЦИИ ДАННЫХ В ОПТИКЕ РАССЕИВАЮЩИХ СРЕД

**М. М. Кугейко, С. А. Лысенко, Д. А. Смунев**

*Белорусский государственный университет, Минск, Беларусь*
*E-mail: kugeiko@bsu.by*

Разработан программный пакет для анализа информативности оптических измерений различных типов аэрозоля (континентальный – фоновый и городской; морской; дымовой и пылевой), а также заведомо несферических частиц – эритроцитов, имеющих в реальности форму, наиболее приближенную к двояковогнутому дискоиду. Универсальность программы обеспечивается возможностью рассмотрения любых комбинаций аэрозольных ОХ, реально осуществляемых на практике.

*Ключевые слова: оптические характеристики; аэрозоль; эритроциты.*

Систематические измерения различных параметров рассеивающих сред (биообъектов, аэрозолей), как в натурных, так и в лабораторных условиях ведутся рядом научных коллективов десятилетия. Получено огромное количество экспериментального материала, выявлены многочисленные статистические зависимости между различными характеристиками данных объектов. Однако получение надёжных данных для требуемых практикой и научными задачами их оптических параметров в большинстве случаев продолжает оставаться проблематичным: биообъекты и аэрозоли чрезвычайно разнообразны и изменчивы по микроструктуре и физико-химическим свойствам, проведение измерений требует больших временных затрат, использования дорогостоящих приборов и систем. Косвенные методы определения микрофизических параметров (МФП) биообъектов, аэрозоля требуют измерения его оптических характеристик (ОХ), использования априорной информации при интерпретации результатов измерений и ее адекватности конкретной ситуации, что далеко не всегда выполнимо.

Априорная информация может быть сформирована в виде общей микрофизической модели, содержащей основные сведения об исследуемых объектах и позволяющей варьировать её характеристики во всём диапазоне возможных изменений. При этом важнейшим является вопрос о возможности отражения этих изменений в измеряемых оптических характеристиках, то есть вопрос об информативности оптических измерений и о том, какие микрофизические параметры биообъектов, аэрозоля могут быть в принципе получены с использованием существующих измерительных систем. Для планирования различных оптических измере-

ний необходимо также решать задачу выбора набора измеряемых ОХ для определения конкретных МФП и оценки потенциальной точности определения последних.

Решение задач оценок информативности исходных оптических измерений предлагается путем получения ансамбля реализаций оптических и микрофизических характеристик рассеивающей среды [1–4] с использованием априорной информации в отмеченном выше виде. Данный ансамбль может быть получен при наличии достаточного большого объема экспериментальных данных по одновременным оптическим и микрофизическим измерениям. Однако проведение комплекса оптических и микрофизических измерений в полном объеме в атмосфере практически не осуществимо и, к тому же, не наблюдается достаточного соответствия оптических и микрофизических данных ввиду сложности интерпретации оптических характеристик относительно микрофизических. Другой подход основывается на экспериментальных сведениях о возможных реальных вариациях микрофизических параметров частиц и последующем расчете необходимых оптических характеристик с “отсеиванием” тех реализаций, которые соответствуют не встречающимся в действительности значениям расчетных оптических и задаваемых микрофизических параметров среды [5]. Преимуществом такого подхода является возможность получения расчетных данных практически обо всех необходимых оптических параметрах, биообъектов, аэрозоля в любом спектральном и угловом диапазонах. Далее рассчитываются ковариационные матрицы оптических и микрофизических характеристик – $\mathbf{D}_{xx}$ и $\mathbf{D}_{yy}$ соответственно, и кроссковариационная матрицы $\mathbf{D}_{xy}$ между этими характеристиками. Используя данные матрицы, можно оценивать погрешности восстановления МФП с использованием метода линейных регрессий [6–8]:

$$\mathbf{x} = \bar{\mathbf{x}} + \mathbf{D}_{xy}\left(\mathbf{D}_{yy} + \mathbf{I}\delta^2\right)^{-1}\left(\mathbf{y} - \bar{\mathbf{y}}\right), \qquad (1)$$

где $\mathbf{x}$ – вектор искомых МФП, $\mathbf{y}$ – вектор измерений ОХ, $\mathbf{I}$ – единичная матрица, $\delta$ – погрешность измерения ОХ. Влияние имеющейся априорной информации на точность интерпретации данных оптических измерений (сопутствующих микрофизических измерений) можно учитывать путем добавления в вектор $\mathbf{y}$ компонент, соответствующих измеряемым МФП.

Формула (1) используется в численных экспериментах по замкнутой схеме для восстановления МФП для множества реализаций параметров модели. Для каждой реализации по регрессионной формуле (1) для заданного набора измеряемых оптических характеристик $Y$, с учетом добавления в их расчетные значения заданных погрешностей измерения, рассчитываются значения МФП которые сравниваются с их заданными

значениями. После перебора всех реализаций вычисляются средние погрешности восстановления МФП.

Данный подход позволяет ранжировать измерения по информативности, решать задачи выбора конкретного набора измерений и оценки их требуемых точностей для определения конкретного МФП, а также оценивать потенциальную точность восстановления МФП с учетом особенностей реальной аппаратуры и имеющейся априорной информации.

Разработан программный пакет для анализа информативности оптических измерений различных типов аэрозоля (континентальный – фоновый и городской; морской; дымовой и пылевой), основанный на вышеизложенных принципах [3]. Универсальность программы обеспечивается возможностью рассмотрения любых комбинаций аэрозольных ОХ, реально осуществляемых на практике. В качестве указанных характеристик рассматривались: объемные коэффициенты ослабления, обратного рассеяния, направленного рассеяния и степень линейной поляризации при рассеянии. Причем указанные характеристики могут измеряться в любой области спектрального диапазона от 0.3 до 15 мкм, как на конкретных длинах волн, так и в заданных спектральных диапазонах. Для индикатрисы и степени поляризации могут быть выбраны любые углы или диапазоны углов. Задавая конкретные измерения, включая их точность, пользователь получает коэффициенты регрессионных соотношений между измеряемыми ОХ и определяемыми МФП аэрозоля и оценки потенциальной точности восстановления последних из оптических измерений, на основе которых можно делать выводы о требованиях к измерениям ОХ.

Для получения указанных регрессий используется база данных, включающая: 1) ансамбли МФП для основных типов (моделей) аэрозолей с использованием известных экспериментальных данных; 2) результаты расчетов ОХ и интегральных МФП для данных ансамблей.

В используемом пакете оптические характеристики аэрозоля рассчитываются в приближении сферических частиц по известным формулам Ми [9]. Такое упрощение обусловлено несколькими причинами. Во-первых, объем экспериментальных данных по форме и внутренней структуре аэрозольных частиц явно недостаточен для построения соответствующих реальности моделей. Во-вторых, методики и алгоритмы расчета оптических характеристик несферических и неоднородных рассеивателей громоздки и имеют лишь ограниченную область применимости [10]. Однако, как отмечено в [10], для хаотически ориентированных сфероидов и цилиндров с умеренным параметром формы $\kappa$ (от 0.5 до 2.0) возникающая при замене разница укладывается в несколько процентов. Отметим также, что для несферических частиц эквивалентные по

площади и по объему радиусы не совпадают, однако для умеренно вытянутых (сплюснутых) сфероидов и цилиндров (с параметром асимметрии $0.5 \le \kappa \le 2$) эта разница не превышает 5% [10], что позволяет рассчитывать объемную концентрацию, не учитывая форму частиц.

Многие реальные рассеивающие дисперсные среды состоят из заведомо несферических частиц. Типичным примером такой среды может служить взвесь нативных (естественных, необработанных) эритроцитов, имеющих в реальности форму, наиболее приближенную к двояковогнутому дискоиду.

Для таких частиц разработан модифицированный программный продукт с открытым исходным кодом ADDA (Д.А.Смунев), реализующий МДД с диполями в виде прямоугольных параллелепипедов [11]. Он может, кроме отмеченных задач диагностики биообъектов, более эффективно использоваться при решении многих других задач оптики рассеивающих сред: экологических, метеорологических, технологических, научных – поскольку позволяет рассчитывать оптические характеристики частиц с учетом особенностей формы рассеивателя. Для сильно сплюснутых или вытянутых рассеивателей достигается ускорение расчетов на несколько порядков. При этом уменьшаются требования к потребляемой памяти вычислительных систем, что дает возможность вести расчет с использованием стандартных пользовательских вычислительных мощностей.

## БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ


1. Кугейко М. М., Лысенко С. А. Лазерная спектронефелометрия аэродисперсных сред. Минск: БГУ, 2012: 208 с.
2. Лысенко С. А. Методы оптической диагностики биологических объектов. Минск: БГУ, 2014: 250 с.
3. Кугейко М. М., Лысенко С. А. Программный пакет для анализа информативности и интерпретации данных аэрозольных оптических измерений // Электроника – инфо, №6, 2009. С.49–52.
4. Ивлев Л. С., Андреев С. Д. Оптические свойства атмосферных аэрозолей. Ленинград: ЛГУ, 1986. 359 с.
5. Лысенко С. А. Методы оптической диагностики биологических объектов. Минск: БГУ, 2014. 230 с.
6. Galushkin A. I. Neural network theory. Berlin: Springer, 2007. 402 p.
7. Колемаев В. А. Теория вероятностей и математическая статистика. Москва. ИНФРА-М, 1997. 302 с.
8. Ligon D., Gillespie J. B., Pellegrino P. M. Aerosol properties from spectral extinction and blockscatter estimated by an inverce Monte-Carlo method // Appl. Opt. 2000. V. 39. N. 24. P.4402–4410.
9. Борен К., Хаффман Д. Поглощение и рассеяние света малыми частицами. Москва: Мир, 1986. 660 с.

10. Зуев В. Е., Наац И. Э. Обратные задачи оптики атмосферы. Ленинград: Гидрометеоиздат, 1990. 286 с.
11. ADDA Rectangular dipole [Electronic resource]. – Mode of access: https://github.com/adda-team/adda/tree/rectangular_dipole. – Date of access: 20.01.2015.

# ПРИМЕНИМОСТЬ ГОМОМОРФНЫХ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

**И. А. Кустов, В. С. Садов**

*Белорусский государственный университет, Минск, Беларусь*
*E-mail: rct.kustov@bsu.by*

Работа рассказывает об основных понятиях и определениях в области гомоморфного шифрования, применениях уже разработанных алгоритмов, а также в ней рассматривается взгляд авторов на гомоморфные криптографических системы, их применимость в различных системах, а также их недостатки.

*Ключевые слова: гомоморфное шифрование; алгоритм; ключ; криптография; безопасность.*

Гомоморфное шифрование, благодаря своим совйствам, является одним из самых перспективных видов шифрования на сегодняшний день. В данной работе авторы ставят перед собой задачу рассказать основные понятия и определения в области гомоморфного шифрования, применения уже разработанных алгоритмов, а также оценить недостатки гомоморфных криптографических систем.

Гомоморфное шифрование — форма шифрования, позволяющая производить определённые математические действия с зашифрованным текстом и получать зашифрованный результат, который соответствует результату операций, выполняемых с открытым текстом. Например, один человек мог бы сложить два зашифрованных числа, а затем другой человек мог бы расшифровать результат, не используя ни одно из них. Гомоморфное шифрование позволило бы объединить в одно целое различные услуги, не предоставляя открытые пользовательские данные для каждой услуги.

Различают частично гомоморфные и полностью гомоморфные криптосистемы. В то время как частично гомоморфная система позволяет производить одновременно только одну из операций — сложение или умножение, полностью гомоморфные криптосистемы поддерживают одновременное выполнение обеих операций. Гомоморфное шифрование является формой шифрования, позволяющей осуществить определённую