# НИИ прикладных проблем математики и информатики: результаты деятельности в области ИКТ

*Ю.С. Харин, Е.Н. Мельникова*
***Научно-исследовательский институт прикладных проблем математики и информатики, г. Минск, Беларусь***
*e-mail: Kharin@bsu.by, MelnikovaEN@bsu.by*

Научно-исследовательский институт прикладных проблем математики и информатики (НИИ ППМИ) создан в 2008 году переименованием Национального научно-исследовательского центра прикладных проблем математики и информатики (ННИЦ ППМИ), организованного по Постановлению Совета Министров Республики Беларусь в 2000 году. Институт является учреждением Белорусского государственного университета и создан с целью развития актуальных научных направлений прикладной математики и информатики. Сайт института: http://apmi.bsu.by.

К основным научным направлениям деятельности НИИ ППМИ относятся:

- Компьютерный анализ данных (многомерный анализ, дискриминантный анализ, кластерный анализ, интеллектуальный анализ данных, анализ временных рядов, прогнозирование);
- Разработка математического и программного обеспечения в области робастного (устойчивого к искажениям модельных предположений) статистического анализа многомерных данных и временных рядов;
- Математическое моделирование физических процессов (моделирование кинетики электронных и атомных процессов в конденсированных средах, моделирование процессов взаимодействия излучения с твердым телом, моделирование элементов квантовых устройств информатики);
- Компьютерные методы в медицинской диагностике;
- Статистический анализ генетических последовательностей;
- Математические и компьютерные методы информационной безопасности;
- Защита информации.

Научные сотрудники Института имеют значительный опыт в области разработки методов и программного обеспечения (ПО) компьютерного анализа данных. Можно отметить участие Института в Европейских исследованиях и академических проектах, финансируемых Программами INTAS, TEMPUS, REAP; выполнение Международных контрактов с компьютерными фирмами из Южной Кореи и Российской Федерации; проведение научно-исследовательских работ в интересах государственных и коммерческих предприятий и организаций Республики Беларусь.

С 2009 года НИИ ППМИ успешно сотрудничает с Институтом математики и информатики Вильнюсского университета, согласно Договору о сотрудничестве. В рамках этого Договора совместно организуются научные

конференции (IX, X International Conferences «Computer Data Analysis and Modeling» и II-VI International Workshops «Data Analysis and Software Systems»), планируются совместные научно-исследовательские работы в области компьютерного анализа данных.

В 2011-2012 г.г. в соответствии с Соглашением между Правительством Республики Беларусь и Правительством Литовской Республики о сотрудничестве в области науки и технологий от 24.01.2008 и в рамках Программы сотрудничества между Государственным комитетом по науке и технологиям Республики Беларусь и Министерством образования и науки Литовской Республики в области науки и технологий от 16.09.2009 в НИИ ППМИ выполнялся проект «Использование легирования германием для увеличения радиационной стойкости приборов на основе кремния». Партнером в этом проекте с Литовской стороны выступал Институт прикладных исследований Вильнюсского университета. Целью совместного проекта была разработка физических основ кремний - германиевой технологии создания полупроводниковых приборов, обладающих повышенной радиационной стойкостью.

Приведем некоторые основные результаты деятельности Института по применению информационно-коммуникационных технологий в различных областях деятельности.

В области медицинской диагностики:

- Методы и алгоритмы для диагностики коронарной ишемической болезни сердца, основанные на параметрическом дискриминантном анализе с использованием статистик, вычисленных по вейвлет коэффициентам, ковариационным функциям и параметрам цепей Маркова.
- Робастные методы дискриминантного анализа для диагностики злокачественных новообразований на основе биохимических показателей крови, позволяющие увеличить точность диагностики по сравнению с классическими решающими правилами.
- Методы, алгоритмы и ПО для пространственно-временного кластерного анализа при определении географического распределения редких болезней. Эти результаты используются для пространственно-временного кластерного анализа злокачественных заболеваний у детей и подростков Беларуси в постчернобыльский период.

В области компьютерного анализа ДНК последовательностей:

- Методы и ПО для распознавания кодирующих участков в ДНК эукариот. Основным недостатком существующих подходов к распознаванию является значительная ошибка при оценке границ кодирующих участков. Подход, разрабатываемый в Институте, имеет целью разработку новых математических моделей для белок-кодирующих участков в ДНК последовательностях эукариот, основанных на многомерном распределении вероятностей фрагментов нуклеотидов, и моделей на основе новых малопараметрических цепей Маркова высокого порядка, разработанных в нашем Институте, а также разработку методов, алгоритмов и ПО для распознавания белок-кодирующих

участков в ДНК последовательностях эукариот на основе построенных математических моделей.

•В области информационной безопасности и защиты информации:

•Блочная криптосистема *BelT*. Алгоритмы шифрования, имитозащиты и хэширования на ее основе.

•Алгоритмы электронной цифровой подписи (ЭЦП) *Bign* (поддерживаются идентификационная подпись и детерминированная выработка подписи).

Идентификационная подпись является новым средством, которое одновременно обеспечивает аутентификацию документа и аутентификацию субъекта, подписавшего этот документ. Обычно алгоритмы выработки ЭЦП являются вероятностными. Это означает, что подписывающий субъект должен использовать надежные случайные числа для построения одноразового личного ключа в процессе создания подписи. Повторение случайных чисел приводит к полной компрометации долговременного личного ключа. Для защиты от неправильного применения случайных чисел в Институте разработан детерминированный алгоритм выработки ЭЦП, в котором одноразовый личный ключ создается с использованием долговременного личного ключа и сообщения, которое должно быть подписано.

•Система широковещательного шифрования *Bee* для защиты данных со спутников.

•Широковещательное шифрование позволяет распространять критические сообщения (например, мультимедийный контент) от одного сервера (спутника) ко многим клиентам. Обратная связь от клиентов отсутствует, и сервер должен организовать отзыв и добавление клиентов только посредством дополнительных ключевых данных, передаваемых вместе с целевыми сообщениями. Протоколы широковещательного шифрования обеспечивают достаточно малый объем дополнительных данных, даже если число клиентов очень велико. Система, разработанная в НИИ ППМИ, реализует данный протокол.

•Криптографическая платформа для Единой системы идентификации и аутентификации физических и юридических лиц.

•Система Национальных стандартов: *СТБ 34.101.27, СТБ 34.101.31, СТБ 34.101.45, СТБ 34.101.60, СТБ 34.101.66*.