О НАУЧНОЙ, НАУЧНО-ТЕХНИЧЕСКОЙ И ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ И АНАЛИЗА ДАННЫХ

Харин Ю. С., Абрамович М. С., Агиевич С. В., Волошко В. А., Палуха В. Ю., Трубей А. И.

НИИ прикладных проблем математики и информатики БГУ,
г. Минск, Республика Беларусь

Ключевые слова: защита информации, анализ данных, криптографическая инфраструктура, информационная система, прогнозирование.

Обеспечение научно-технологической безопасности Республики Беларусь невозможно без двух приоритетных направлений научной, научно-технической и инновационной деятельности: 1) обеспечение информационной безопасности страны на основе защиты информации в информационных системах глобального и локального уровней; 2) разработка систем компьютерного анализа больших данных в целях построения оптимальных оценок, решений и прогнозов.

Одним из адекватных ответов на вызовы XXI в. в Республике Беларусь явилось своевременное создание 18 августа 2000 г. на базе Белорусского государственного университета нового научно-исследовательского учреждения «НИИ прикладных проблем математики и информатики» (НИИ ППМИ) специальным постановлением Совета Министров Республики Беларусь «в целях развития и координации в Республике Беларусь теоретических и прикладных научных исследований в области криптографической защиты информации, компьютерного моделирования и анализа данных». Отметим, что согласно этому постановлению поручено «ГКНТ и Минфину при формировании бюджета на 2001 и последующие годы предусматривать в установленном порядке выделение бюджетных ассигнований для финансирования научных исследований по разработке и совершенствованию методов, алгоритмов и компьютерных систем сертификационных испытаний средств криптографической защиты информации (СКЗИ), используемых и проектируемых в республике».

НИИ ППМИ благодарен Государственному комитету по науке и технологиям Республики Беларусь за поддержку становления и развития института, позволившую получить важные для страны результаты, представленные ниже.

Результаты в области защиты информации.

1. Создана и развивается национальная научная школа по криптологии — науке о математических и компьютерных методах защиты информации [1]. Подготовлено более 25 кандидатов наук и 2 доктора наук. Результаты внедрены в системах защиты информации, обеспечивающих информационную безопасность электронного документооборота в стране.

2. Разработана система криптографических алгоритмов и протоколов, которая включает: блочный шифр Belt; режимы шифрования, имитозащиты и хэширования на основе Belt; систему электронной цифровой подписи Bign на основе эллиптических кривых; транспорт ключа на платформе Bign; криптографическую sponge-функцию Bash-f; алгоритмы хэширования и программируемые криптографические алгоритмы на основе Bash-f; протоколы формирования общего ключа Bake на основе эллиптических кривых; алгоритмы генерации псевдослучайных чисел и др.

Перечисленные криптографические механизмы представлены в разработанных в НИИ ППМИ следующих национальных стандартах, которые широко применяются в информационных системах страны, составляют основу отечественной криптографической инфраструктуры:

– СТБ 34.101.31-2020 «Информационные технологии и безопасность. Криптографические алгоритмы шифрования и контроля»;

– СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых»;

– СТБ 34.101.47-2017 «Информационные технологии и безопасность. Алгоритмы генерации псевдослучайных чисел»;

– СТБ 34.101.60-2014 «Информационные технологии и безопасность. Алгоритмы разделения секрета»;

– СТБ 34.101.66-2014 «Информационные технологии и безопасность. Протоколы формирования общего ключа на основе эллиптических кривых»;

– СТБ 34.101.77-2020 «Информационные технологии и безопасность. Криптографические алгоритмы на основе sponge-функции»;

– СТБ 34.101.27-2022 «Информационные технологии и безопасность. Средства криптографической защиты информации. Требования безопасности»;

– СТБ 34.101.78-2019 «Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей»;

– СТБ 34.101.79-2019 ««Информационные технологии и безопасность. Криптографические токены»; с помощью токена его владелец может аутентифицироваться перед удаленными прикладными системами, вырабатывать ЭЦП, расшифровывать ключи защиты данных; на токене хранятся идентификационные данные владельца, фактически токен представляется собой ID-карту гражданина;

– СТБ 34.101.87-2022 «Информационные технологии и безопасность. Инфраструктуры аутентификации».

3. Разработано криптографическое программное обеспечение, в котором поддержаны все базовые криптографические механизмы и часть высокоуровневых: криптографическая библиотека Bee2 и пакеты Bee2evp и Bee2j, которые интегрируют Bee2 в среды OpenSSL и Java. Разработанное программное обеспечение является открытым, оно используется разработчиками СКЗИ республики.

4. Разработаны основы теории оценок качества источников случайности (энтропии) — генераторов случайных и псевдослучайных последовательностей, которые широко используются в компьютерных системах защиты информации для генерации паролей, ключевой информации и других целей.

5. Разработаны и зарегистрированы Программный комплекс «Энтропийный анализ дискретных последовательностей» (ЭАДП), позволяющий оценивать качество выходных последовательностей криптографических генераторов на основе энтропийных функционалов Шеннона, Реньи, Тсаллиса, и Компьютерный практикум по криптографической защите информации для учебного процесса по специальности «Компьютерная безопасность».

Результаты в области анализа данных.

1. Разработаны основы теории робастного (устойчивого к искажениям модели наблюдений) статистического анализа данных и распознавания образов, позволившей решить новые прикладные задачи в технике, медицине и экономике [2].

2. Разработан Программный комплекс «Оценивание показателей надежности и долговечности автотранспортных средств», который используется в ОАО «МАЗ» для оценки надежности деталей, узлов и агрегатов по опытным партиям автотранспортных средств до начала серийного выпуска в целях предотвращения появления массовых неисправностей, а также для прогнозирования надежности разрабатываемых моделей автотранспортных средств.

3. Совместно с РНПЦ онкологии и медицинской радиологии им. Н. Н. Александрова разработана Экспертная система диагностики злокачественных новообразований на основе показателей биохимического тестирования крови с использованием робастных статистических решающих правил и Инструкция по ее применению, утвержденная в Минздраве. Экспертная система диагностики внедрена в областных онкодиспансерах и Минском городском клиническом онкодиспансере.

4. Разработана Программная система эконометрического моделирования и прогнозирования для оценки вариантов денежно-кредитной политики Национального банка Республики Беларусь.

Список литературы:

1. Харин, Ю. С. Криптология / Ю. С. Харин, С. В. Агиевич, Д. В. Васильев, Г. В. Матвеев. — Минск: БГУ, 2014. — 512 с.

2. Kharin, Yu. Robustness in Statistical Forecasting / Yu. Kharin. — Heidelberg/New York/ Dordrecht/ London: Springer, 2013. — 356 p.