ИССЛЕДОВАНИЯ ПО ПРОЕКТАМ, ПОДДЕРЖАННЫМ СОВЕТОМ ПО ГРАНТАМ ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Грант Президента РФ МК-1647.2020.9 «Методы и средство создания онтологий и их шаблонов на основе преобразований электронных таблиц в контексте обработки больших данных»

Руководитель проекта – к.т.н. Н.О. Дородных

Метод формирования онтологий в формате OWL/RDF на основе извлечения данных из исходных произвольных электронных таблиц в формате MS Excel;

метод формирования паттернов онтологического проектирования на основе трансформации концептуальных моделей;

мпрототипы модулей поддержки методов.

Стипендия Президента РФ молодым ученым и аспирантам СП-3545.2019.5 «Применение высокопроизводительных вычислений к построению алгебраических атак на криптографические хеш-функции»

Руководитель проекта – И.А. Грибанова

В 2020 году были построены новые атаки, использующие метод специальных функций и алгоритмы поиска инверсных лазеек (Inverse Backdoor Set, IBS), на хеш-функции вида MD4-k до k=48 включительно (k – число шагов базового алгоритма сжатия), а также на функции MD5-k до k=32. Основная новизна результатов состоит в использовании для поиска IBS эволюционных алгоритмов, а также в применении для оценки трудоемкости конкретной атаки меры, выраженной в числе инструкций процессорного кэша (для получения значений данной меры использовался программный инструмент Valgring). Еще один результат состоит в новом подходе к генерации ограничений, ослабляющих исходную задачу обращения. Конкретно, для получения специальных функций, к обращению которых сводится поиск прообразов рассматриваемой хеш-функции, организуется перебор возможных вариантов сочетаний ослабляющих ограничений. Перебор осуществляется при помощи эволюционного алгоритма, обходящего булев гиперкуб, в котором каждая точка задает конкретный набор ослабляющих ограничений. После того как множество перспективных наборов ограничений построено, эти наборы анализируются дополнительно (как правило, вручную), и из них выбирается несколько наборов, которые в дальнейшем используются для построения IBS атак. Применение этого алгоритма к функции сжатия алгоритма MD5 дало следующие результаты. Для первых двух раундов функции сжатия (то есть для 32 шагов) MD5 были найдены ослабляющие ограничения, давшие функции вида g:{0,1}^128 --> {0,1}^128. Для этих функций были построены IBS-атаки, лучшая из которых имеет оценку сложности 9,17x10^39 инструкций кэша процессора, тогда как реализация метода грубой силы для обращения MD5-32 потребует 4,3x10^43 инструкций.

Стипендия Президента РФ молодым ученым и аспирантам СП-3545.2019.5 «Разработка комплекса алгоритмов для поиска декомпозиций трудных примеров задачи булевой выполнимости с применением методов комбинаторной оптимизации»

Руководитель проекта – С.Е. Кочемазов

В рамках стипендии Совета по грантам Президента Российской Федерации № СП-2017.2019.5 был получен ряд результатов по комплексу направлений, связанных с разработкой и применением SAT-решателей для решения широкого спектра задач. Так, были разработаны несколько эвристик, нацеленных на повышение средней производительности современных SAT-решателей на широких классах тестовых задач. Помимо этого, были разработаны эвристики для реорганизации последовательности обработки точек в окрестностях, просматриваемых алгоритмами локального поиска в рамках их применения к оптимизации блэкбокс-функций, оценивающих трудоемкость решения конкретных трудных примеров SAT. Все полученные результаты опубликованы в трудах российских и зарубежных международных конференций и рейтинговых журналах.