ЮБИЛЯРЫ

Людмиле Климентьевне БАБЕНКО – 75 лет

Людмила Климентьевна Бабенко – доктор технических наук (1994), профессор (1999), действительный член Российской академии естествознания (2010), член-корреспондент Российской академии естественных наук (2006). Работает в университете (ТРТИ, ТРТУ, ЮФУ) штатным сотрудником с 1970 года по настоящее время на должностях: м.н.с., с.н.с., зав. лабораторией НИИ МВС, профессор кафедры БИТ, директор НОЦ «Современные технологии безопасности».

Основные научные результаты за последние 5 лет. Разработаны и исследованы параллельные алгоритмы оценки криптографической стойкости защиты информации. Рассмотрены возможность и базовые алгоритмы применения дифференциального криптоанализа (ДК) к блочным и поточным шифрам. Для реализации параллельных алгоритмов анализа блочных шифров на основе метода ДК использовалась библиотека MPI. При построении программных реализаций методов асимметричной криптографии использовались библиотека распределенных вычислений Open MPI, диспетчер заданий SLURM, библиотека работы с числами произвольной длины NTL, технология CUDA. Полученные экспериментальные данные для параллельных алгоритмов отражают зависимость скорости вычислений от используемого числа процессоров и способа распределения данных. Экспериментальные данные отражены в опубликованных статьях и монографиях. Разработаны рекомендации по использованию симметричных и асимметричных алгоритмов шифрования и методов их анализа, а также по использованию разработанных алгоритмических и программных средств.

Проведено исследование стойкости современных функций хэширования. В частности, рассмотрены пять новых функций хэширования, которые являются финалистами конкурса SHA-3, а именно: Skein, Blake, Grostl, JH, Keccack. Все пять функций программно реализованы, полученные реализации использованы для определения возможности проведения анализа стойкости данных функций. Дана подробная классификация существующих на сегодняшний день функций хэширования, подробно рассмотрены различные схемы построения хэш-функций. Рассмотрены подходы к анализу ключевых и бесключевых функций хэширования. Разработаны и реализованы последовательные и параллельные алгоритмы анализа стойкости.

Разработан новый метод классификации образцов вредоносного ПО на основе анализа динамического графа исполнения. Метод основан на сопоставлении базовых блоков и формы графа. По сравнению с представленными в научной печати методами статической классификации вредоносных образцов разработанный метод позволяет выполнять классификацию упакованных и полиморфных вредоносных программ. При этом время анализа данных одной пары образцов примерно в 10 раз меньше, чем в существующих методах на основе динамического анализа. Разработан новый метод определения близости вредоносных программ на основе наибольшей общей подпоследовательности (Longest Common Subsequence), позволяющий определять не только идентичность вредоносных образцов, но и модификации одного и того же полиморфного и метаморфного образца.

Разработана программная система активного поиска и анализа вредоносного программного обеспечения (активная система-ловушка). Отличием от существующих систем являются разработанные алгоритмы релевантного поиска вредоносного программного обеспечения в Интернете. Предлагаемая система опирается на гипотезу о связности Web-страниц с близкой тематикой (в данном случае – вредоносных страниц) и возможности поиска множества таких страниц путем анализа связей в некотором небольшом их подмножестве.

Л.К. Бабенко руководит 5 аспирантами. Под ее руководством 10 аспирантов получили звание кандидата технических наук. Подготовлены и читаются курсы по следующим дисциплинам: «Криптографические методы защиты информации», «Программно-аппаратная защита информации», «Анализ безопасности протоколов».

Награды. Медаль ФСТЭК России «За укрепление государственной системы защиты информации»; грамота ФСТЭК России за активное участие в решении задач в области защиты информации в интересах ФСТЭК России и личный вклад в организацию и подготовку специалистов в области обеспечения информационной безопасности Российской Федерации; благодарность Минобрнауки за высокий профессионализм в проведении экспертизы заявок, поданных в 2011 г., 2013 г. в рамках конкурса на получение гранта Правительства Российской Федерации для государственной поддержки научных исследований, проводимых под руководством ведущих ученых в российских образовательных учреждениях высшего профессионального образования, научных учреждениях государственных академий наук и государственных научных центрах Российской Федерации; нагрудный знак «Почетный работник высшего профессионального образования Российской Федерации».

Л.К. Бабенко – эксперт РФФИ, эксперт РНФ, эксперт Минобрнауки, член редколлегии журналов «Известия ЮФУ. Технические науки», «Вопросы кибербезопасности».