# РЕАЛИЗАЦИЯ РАСПРЕДЕЛЕННОЙ АТАКИ НА КЛАССИЧЕСКИЕ АССИМЕТРИЧНЫЕ ШИФРЫ

Бережный А.В., *аспирант*, Коломеец А.В., *студент*

На современном этапе развития технологий передачи данных достаточно актуальным является вопрос защиты передаваемых данных. Целью данной работы является обзор существующих систем сбора и криптографического анализа данных, а так же реализация собственной системы атаки на классические ассиметричные шифры.

Особенностью данной работы является отказ от традиционной последовательной модели обработки данных и переход к параллельной модели.

В целом работа должна быть выполнена с учетом следующих требований:

- реализация параллельной модели обработки данных;
- использование легко портируемых языков программирования, напр. Python.

В ходе выполнения работы был выполнен обзор архитектуры комплекса критоанализаPyrit. Данный комплекс вызвал интерес тем, что позволяет создавать и обрабатывать массивные базы данных пред-вычислительной части IEEE 802.11 WPA/WPA2-PSKфазы аутентификации. Используя вычислительнуюмощностьмногоядерныхи других платформ через ATI-Stream, Nvidia CUDA, OpenCLand VIA Padlock, это - в настоящий момент, безусловно, самая мощная атака против одного из наиболее используемых протоколов системы защиты в мире.[1]

Анализ архитектуры комплекса дал подоснову для разработки вычислительной части атаки на ассиметричные шифры. В перспективе необходимо внедрение системы распределения и балансировки нагрузки между вычислительными узлами.

1. http://pyrit.wordpress.com/about/