**BC/NW 2019 № 1 (34):11.1**

**ОПТИМИЗАЦИЯ АЛГОРИТМОВ СИММЕТРИЧНОГО БЛОЧНОГО ШИФРОВАНИЯ С ПРИМЕНЕНИЕМ ГРАФИЧЕСКОГО УСКОРИТЕЛЯ**

Прокофьев М.А., Филатов А.В.

В современном мире информация играет важную роль в жизни человека. Ежедневно в мире обрабатываются терабайты данных, шифрование которых является довольно непростой задачей.

Среди всех разновидностей алгоритмов шифрования особую роль играет класс симметричных блочных шифров. Сходство процедур шифрования и дешифрования, высокая степень обеспечения защиты данных и производительности, по сравнению с другими классами, обеспечили ему большую популярность и широкое распространение[1].

Большинство ПО, реализующие данные алгоритмы, только в редких случаях используют весь доступный потенциал оборудования, в частности различные графические ускорители. По этой причине процесс шифрования может занимать продолжительное время, что является неприемлемым при высокоскоростной обработке данных, и делает ускорение данного процесса актуальной задачей.

Именно с целью решения этой задачи автором было проведено исследование, в рамках которого были проанализированы существующие алгоритмы блочного шифрования (*AES* и ГОСТ Р 34.12-2015) [1] [2], а также разработаны специальные библиотеки, реализующие эти алгоритмы с использованием технологий параллельного программирования (в частности *OpenCL)* [3].

С примерами полученных в рамках исследования показателей скорости шифрования файла размером 1024 МБ можно ознакомиться ниже:

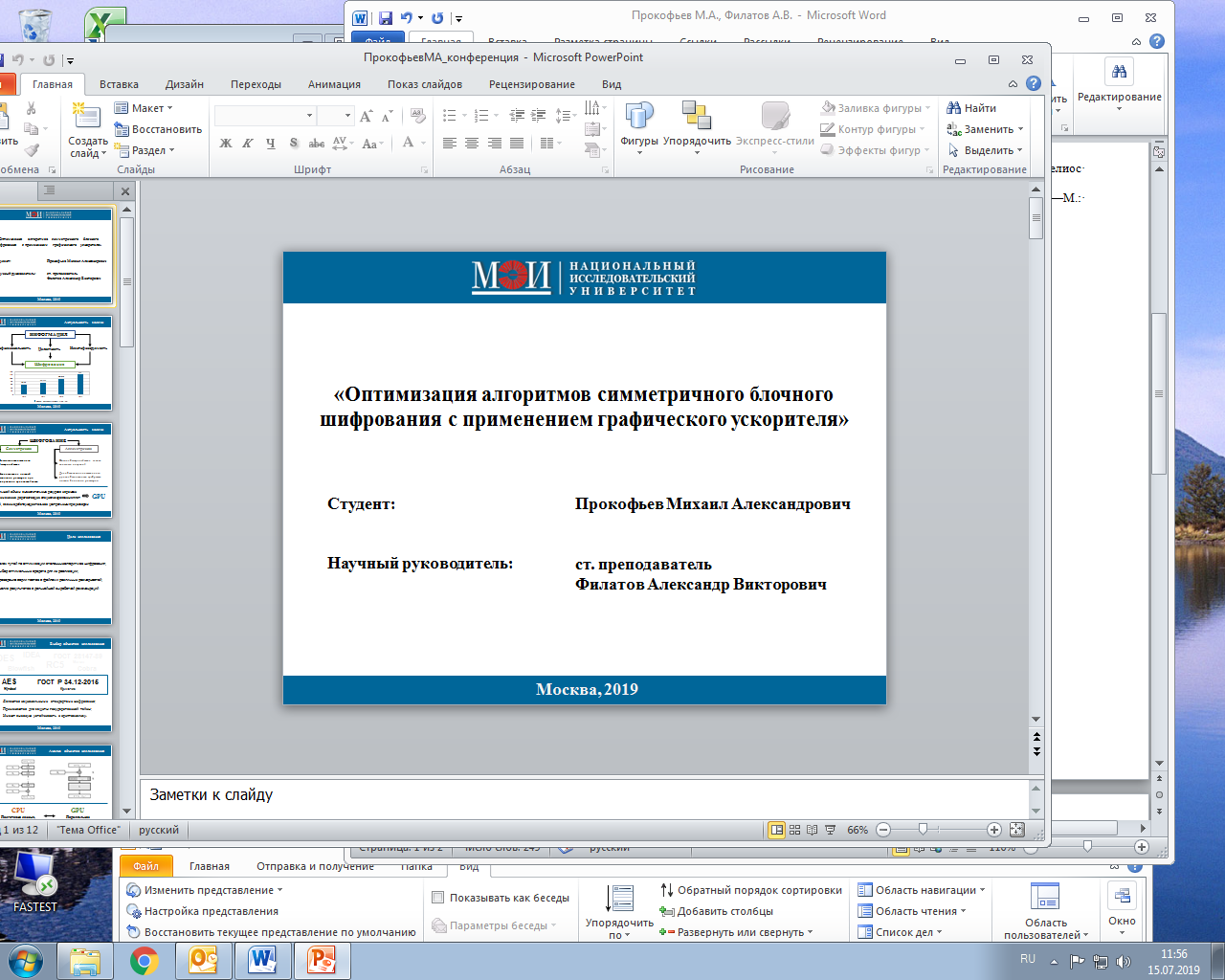
Таблица 1

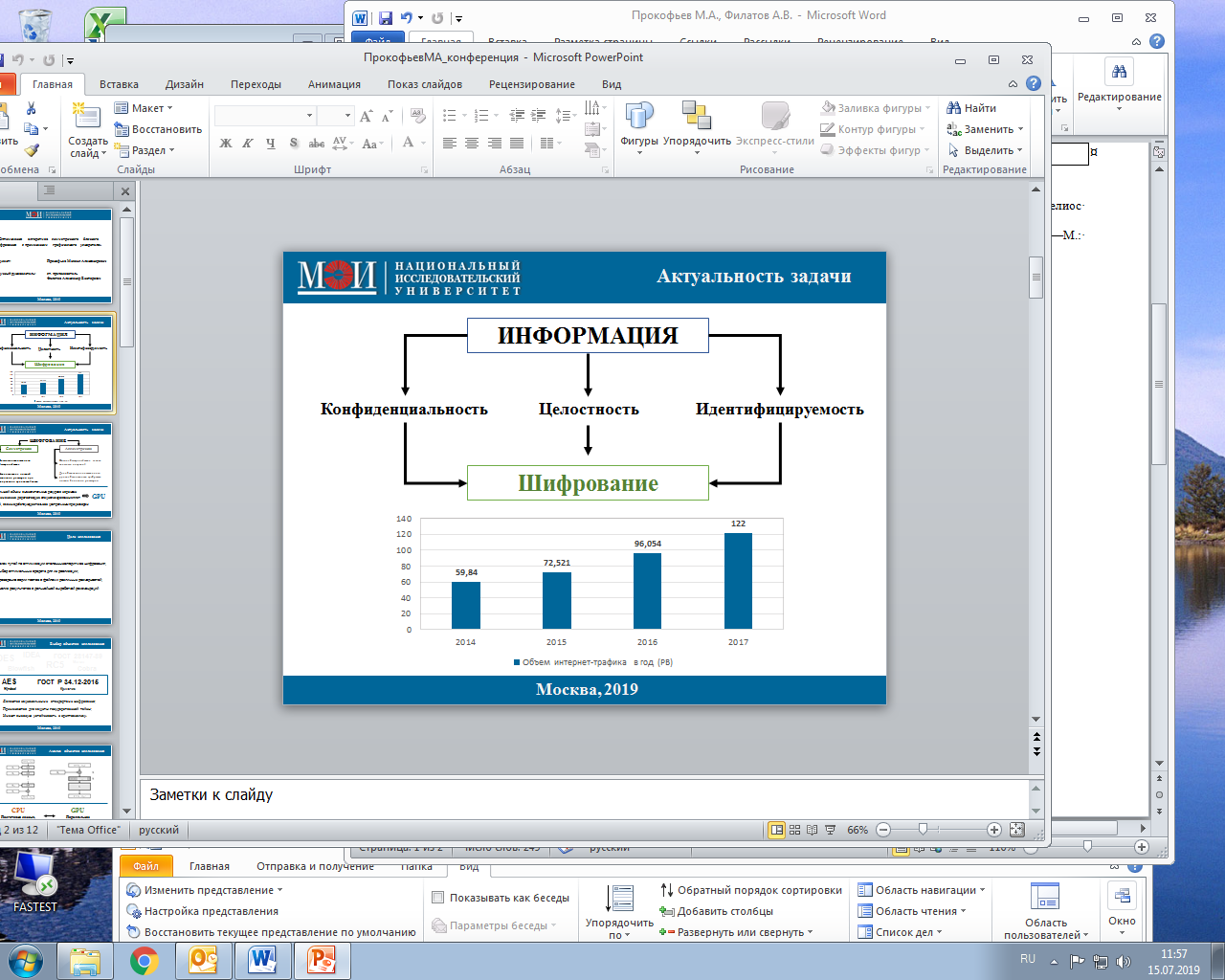
**Скорость шифрования данных в МБ/c алгоритмами *AES* и ГОСТ**

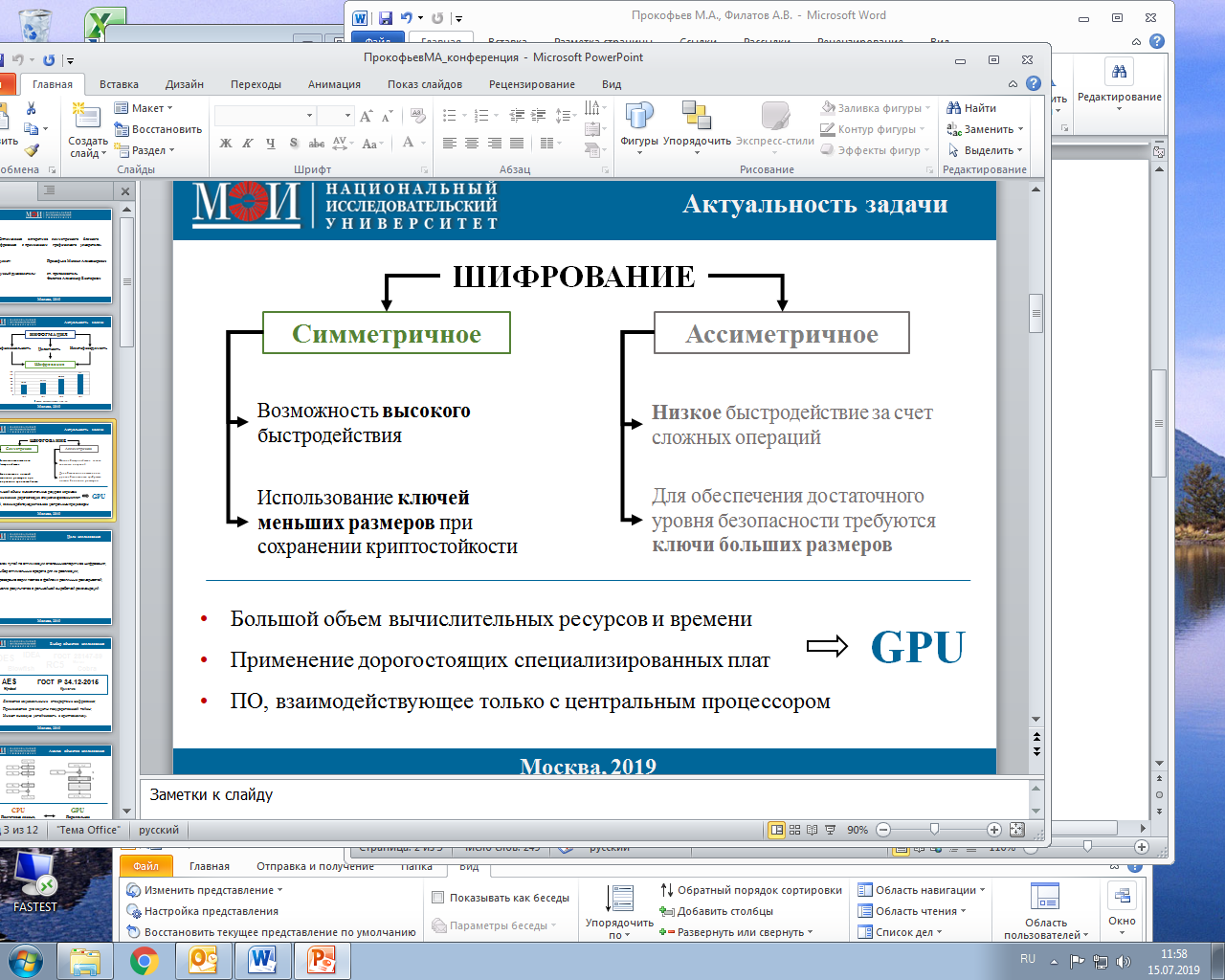
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***AES-256*** | | | **ГОСТ Р 34.12-2015** | | |
| *CPU* | *OpenCL-CPU* | *OpenCL-GPU* | *CPU* | *OpenCL-CPU* | *OpenCL-GPU* |
| 35,23 | 127,680798 | 436,1158433 | 3,30 | 36,70514015 | 109,2499733 |

**Литература**

1. **Современные алгоритмы блочного шифрования и методы их анализа.** Л. К. Бабенко, Е. А. Ищукова. – М.: Гелиос АРВ, 2006. – 376 с.
2. **ГОСТ Р 34.12—2015.** Информационная технология. Криптографическая защита информации. Блочные шифры. —М.: Стандартинформ, 2015.— 6 с.
3. **OpenCL Overview**. URL: <https://www.khronos.org/opencl/>







**ЦЕЛИ** **ИССЛЕДОВАНИЯ**

