Моделирование работы высокоскоростного шифратора

Кирякина Светлана Алексеевна

Студент

Национальный исследовательский ядерный университет «МИФИ», Институт интеллектуальных кибернетических систем, Москва, Россия

E-mail: s.kiryakina@grcc.it

Высокоскоростные шифраторы (ВШ) используются при обработке больших объемов данных. В следствии увеличения мощности технических устройств и повышения пропускной способности каналов связи возрастает скорость обработки информации. Используемое оборудование защиты информации, а именно, шифрования, которое применяется в сферах работы с конфиденциальной информацией, должно соответствовать увеличивающимся потребностям общества. Применение методов моделирования позволяет обосновать методики разделения нагрузки между аппаратными низкоскоростными шифраторами (НШ) и схемы их соединения для получения ВШ с большим быстродействием.

В настоящей работе реализовано построение имитационные модели ВШ с использованием значений параметров шифраторов и алгоритмов синхронизации. Изучены варианты реализации ВШ: сетевые и проходные шифраторы [1, 2]. Моделирование ВШ выполнено для сетевого шифрования на основе алгоритма «Магма» стандарта ГОСТ Р 34.12–2015 [3, 4]. При моделировании ВШ на основе анализа поведения сетевого трафика выбрано распределение Гаусса.

В [5] был предложен метод синхронизации на основе применения задержки выхода пакетов в шифраторе. В настоящей работе проведен сопоставительный анализ алгоритмов синхронизации, применение которых необходимо для обеспечения корректной работы ВШ. На основе полученных результатов предложено использование упорядочивающей очереди для синхронизации пакетов на выходе ВШ, получена формула расчета размера упорядочивающего буфера. Построены модели ВШ в системе имитационного моделирования GPSS World. Анализ отчетов позволил сделать вывод о рекомендованном использовании упорядочивающего буфера для синхронизации следования пакетов.

Таким образом, на основе применения разработанных моделей ВШ возможно качественно оценить функциональность шифратора и целесообразность распределения нагрузки между несколькими НШ

для повышения общей производительности системы защищенного обмена данными.

Литература

1. Аппаратные шифраторы:
   http://www.osp.ru/pcworld/2002/08/163808/
2. Епишкина А. В., Кирякина С. А. Имитационное моделирование как инструмент для построения высокоскоростного шифратора // Безопасность информационных технологий. 2015, 3. С. 44–51.
3. ГОСТ Р 34.13–2015: стандарт строгого режима:
   http://www.itsec.ru/articles2/crypto/
   gost-standart-strogogo-rezhima
4. ГОСТ Р 34.12–2015. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ. 2015.
5. Епишкина А. В., Кирякина С. А. Об имитационном моделировании работы высокоскоростного шифратора // Материалы 24-ой научно-технической конференции «Методы и технические средства обеспечения безопасности информации», Санкт-Петербург, Россия, 2015. С. 141–143.