A. V. Epishkina, S. A. Kiryakina

The Possibility of Using Simulation Systems for the Development of a High-speed Encipherer

Key words: encipherer, model, simulation modelling

The paper presents the investigation of a possibility of using simulation systems for the development of a high-speed encipherer. The systematization of methods for constructing a high-speed encipherers and techniques to simulate network processes was done and the choice of General Purpose Simulation System (GPSS) as the modeling system was established. The main result of the work was the conclusion allowed to utilize simulation modelling to construct a high-speed encipherer.

А. В. Епишкина, С. А. Кирякина

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ СИСТЕМ
ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ДЛЯ РАЗРАБОТКИ
ВЫСОКОСКОРОСТНОГО ШИФРАТОРА

Жизнь современного общества трудно представить без повсеместного применения информационных технологий. Массовое использование компьютеров позволяет решать задачу автоматизации обработки информации, поднимая другую проблему — проблему информационной безопасности. Алгоритмы защиты информации, а именно шифрования, можно реализовать программным, аппаратным и программно-аппаратным способами. Очевидно, что на критически важных объектах информатизации предпочтение отдается аппаратным методам криптографической защиты информации.

Настоящая работа посвящена исследованию возможности применения систем моделирования для повышения скоростных характеристик шифраторов. Методами имитационного моделирования, без проведения дорогостоящего эксперимента, предполагается обосновать методику разделения нагрузки между низкоскоростными шифраторами, а также схему их соединения для построения высокоскоростного шифратора (рис. 1, где НШ — низкоскоростной шифратор, ВШ — высокоскоростной шифратор, f — разбиение функции шифрования на подзадачи для распределения между НШ, i находится в интервале от 1 до n, где n — количество НШ).

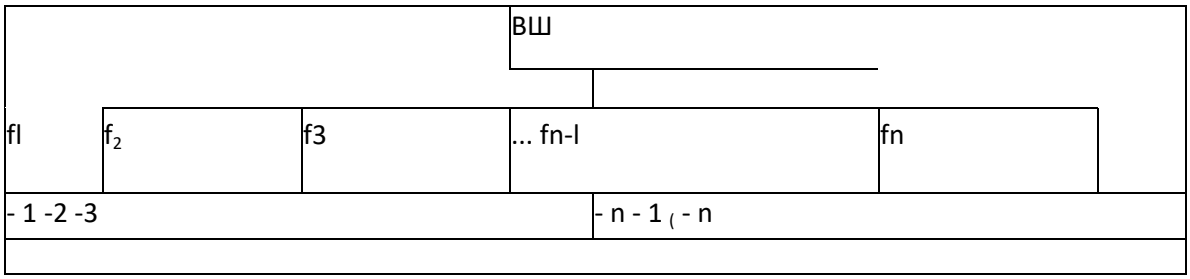

Рис. 1. Схема высокоскоростного шифратора на основе параллельного соединения нескольких низкоскоростных шифраторов

Авторами проведена классификация шифраторов по скорости обработки данных, проанализированы их реализации, основные свойства и характеристики, проведено исследование принципов работы шифратора в целом, выделены его основные и дополнительные блоки. Полученные результаты позволяют сделать вывод о том, что наибольшей скоростью обработки данных обладает шифратор Senetas CN6 [1]. Однако данное устройство реализует алгоритм шифрования AES [2], следовательно, актуальной задачей является изучение возможности достичь таких же скоростей для моделируемого высокоскоростного шифратора, реализующего алгоритмГОСТ 28147-89 [3].

Очевидно, крайне нецелесообразно проведение дорогостоящего эксперимента для определения параметров схемы соединения низкоскоростных шифраторов и оценки нагрузки на каждый узел. Анализ показывает, что для решения поставленной задачи наилучшим образом подходит аппарат имитационного моделирования. Однако имитационное моделирование не может давать абсолютный результат, и необходимо рассмотреть вопрос об оценке погрешностей и выборе определенных условий, при которых достижим тот или иной результат.

Для рационального использования ресурсов в процессе моделирования следует разрабатывать план, определяющий не только контрольные точки мероприятия, порядок статистического анализа результатов, но и в целом успешное выполнение задания и конкретных его этапов. В зависимости от точности полученного результата, определяемого дисперсией случайного фактора, следует говорить о степени доверия к полученным материалам, а также о возможных условиях и ограничениях при применении этой модели. Требуемую степень точности можно задать в различных формах: в виде доли стандартного отклонения, в процентах от среднего значения, в абсолютных значениях и т. д. Существующие погрешности вычислений можно уменьшить, например, методом повторения эксперимента, более точным способом формирования случайных выборок.

Для качественного использования результатов имитационного моделирования и адекватного проведения эксперимента необходимо учитывать возможные недостатки любой модели, заключающиеся в том, что модель может содержать несущественные переменные или не содержать существенных переменных, а также в том, что одна или более существенных переменных могут быть оценены или представлены неточно.

Проведенный анализ различных сред имитационного моделирования позволяет выбрать систему моделирования GPSS , которая в наибольшей степени подходит для решения поставленной задачи по своим целевым и алгоритмическим особенностям. также ее преимуществом является доступность среды разработки и большая популярность, благодаря которой существует достаточное количество материалов и примеров, иллюстрирующих решение практических задач.

В процессе выполнения работы были получены следующие основные результаты:

- систематизированы подходы к построению высокоскоростных шифраторов;
- предложена методика разработки высокоскоростного шифратора;
- разработана классификация методов моделирования, на основе которой был обоснован выбор метода имитационного моделирования для дальнейших исследований;
- систематизированы современные системы имитационного моделирования;
- обоснован выбор системы GPSS для дальнейшей работы, сформулированы ее преимущества и недостатки;
- обоснована возможность применения систем имитационного моделирования для разработки высокоскоростного шифратора, основанного на параллельном соединении низкоскоростных шифраторов.

В рамках дальнейших исследований планируется произвести необходимые расчеты для последующего моделирования высокоскоростного шифратора, определить параметры используемых устройств и сети, а также уточнить предложенную схему моделируемого устройства.

СПИСОК ЛИТЕРАТУРЫ:

1.Новый сетевой шифратор компании Senetas позволяет защищать данные на скорости до 100 Гб/с. [Электронный ресурс]. URL: http://www.osp.ru/resources/releases/?rid=11006 (дата обращения: 09.12.2014).

2.Advanced Encryption Standard. Federal Information Processing Standards Publications. FIPS-197. 2001.

3.ГОСТ 28147—89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введ. 1990-30-06. М.: ИПК Издательство стандартов, 1990. — 28 с.

REFERENCES:

1.Novyi setevoi shifrator kompanii Senetas pozvolyaet zashchishchat’ dannye na skorosti do 100 Gb/s. [Electronic resource]. URL: http://www.osp.ru/resources/releases/?rid=11006 (date of the request: 09.12.2014).

2.Advanced Encryption Standard. Federal Information Processing Standards Publications. FIPS-197. 2001.

3.GOST 28147—89. Systemy obrabotki informatsii. Zashchita kriptorgaficheskaya. Algoritm kriptograficheskoro preobrazovania. Vved. 1990-30-06. M.: IPK Izdatel’stvo standartov, 1990. — 28 p.