A.V. Epishkina, S.A. Kiryakina

The Modeling of A High-Speed Encipher

Keywords: encipher, model, simulation modelling.

The paper presents options of the implementation of high-speed encipher and gives an analyze of models high-speed encipher. The report considers the main characteristics of the encipher which affect on the speed of the data processing; ways of modeling the input stream and sync final device encryption.

А.В. Епишкина, С.А. Кирякина

О МОДЕЛИРОВАНИИ ВЫСОКОСКОРОСТНОГО ШИФРАТОРА

Введение

Информационные технологии являются неотъемлемой частью жизни современного общества. Массовое использование компьютеров позволяет решать задачу автоматизации обработки информации, поднимая другую проблему – проблему защиты информации.

Один из способов реализации алгоритмов защиты информации, а именно: шифрования, аппаратный – более надежный, а также исключающий какое-либо стороннее вмешательство в процесс шифрования.

Высокоскоростные шифраторы (ВШ) используются при обработке больших объемов данных. Методами моделирования возможно обоснование методики разделения нагрузки между аппаратными низкоскоростными шифраторами (НШ) и схемы их соединения для получения ВШ. Анализируя построенные модели, можно качественно оценить функциональность шифратора и целесообразность распределения нагрузки между несколькими НШ для повышения общей производительности системы защищенного обмена данными.

С увеличением мощностей техники и повышением пропускной способности каналов связи растет скорость обработки информации. Используемое оборудование защиты информации, а именно: шифрования, которое применяется в сферах работы с конфиденциальной информацией, должно соответствовать увеличивающимся потребностям общества. Поэтому работа над поставленной темой позволит решить важную задачу в области информационных технологий и защиты информации.

Авторами проанализированы основные характеристики шифраторов, влияющие на скорость работы с данными, исследованы способы моделирования входного потока и синхронизации конечного устройства шифрования, рассмотрена зависимость скорости обработки данных от алгоритма шифрования, произведено моделирование ВШ и анализ полученных моделей.

Варианты реализации ВШ

В ходе исследования было рассмотрено высокоскоростное шифрование с использованием проходных шифраторов, работающих на PCI-порту компьютера [1] (рис.1), и шифрование между удаленными устройствами (рис. 2).

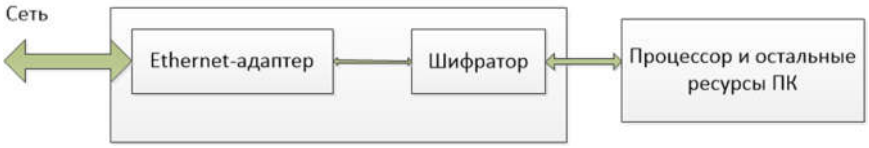


Рис. 1. Проходной шифратор

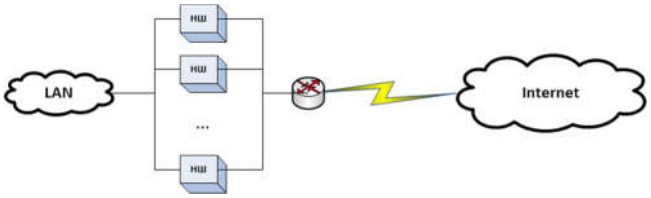


Рис. 2. Сетевой ВШ

Проходной шифратор [1] – аппаратный шифратор, в котором шифратор и сетевой адаптер Ethernet выполнены в качестве одной PCI-платы. Его достоинство в том, что он полностью контролирует весь информационный обмен, а обойти его как изнутри, так и снаружи невозможно.

В работе [2] приведено описание основных блоков аппаратного шифратора, работающего на PCI-порту компьютера пользователя. Такое устройство – средство криптографической защиты информации (СКЗИ) – помимо шифрования, предоставляет ряд дополнительных возможностей, среди которых – идентификация и аутентификация пользователя, контроль целостности файлов, функция датчика случайных чисел, генерация электронной цифровой подписи и т.д. [3]. То есть такой шифратор работает с данными в пределах одного персонального компьютера (ПК).

Необходимо ли высокоскоростное шифрование в масштабах обработки данных на одном ПК или для решения задачи защищенного обмена данными одного ПК с сетью? Будут ли затраты на дополнительное оборудование сопоставимы с полученной выгодой в эксплуатации? Установка плат расширения, содержащих несколько портов PCI, и параллельная коммутация нескольких СКЗИ на каждом компьютере, выполняющем высокоскоростное шифрование, – дорогостоящий процесс, который, вероятнее всего, будет невыгоден.

Также авторами рассмотрено сетевое шифрование. Под сетевым шифрованием подразумевается передача зашифрованной информации между удаленными узлами сети [4]. В настоящей работе рассматривается сетевое шифрование на сетевом и на канальном уровне сетевой модели OSI, шифрование трафика происходит на отдельном устройстве, не на PCI-порту ПК. Для сетевых шифраторов, работающих на втором уровне размер кадров будет варьироваться в интервале 64–1518 байт – диапазон возможных размеров кадра Ethernet. Для шифраторов, работающих на третьем уровне, размер пакета может достигать 65535 байт, размер заголовка пакета – 20 байт. Эти параметры используются при моделировании потока поступающих данных на вход ВШ (кадров либо пакетов в зависимости от уровня моделирования ВШ).

Работа ВШ с входными данными

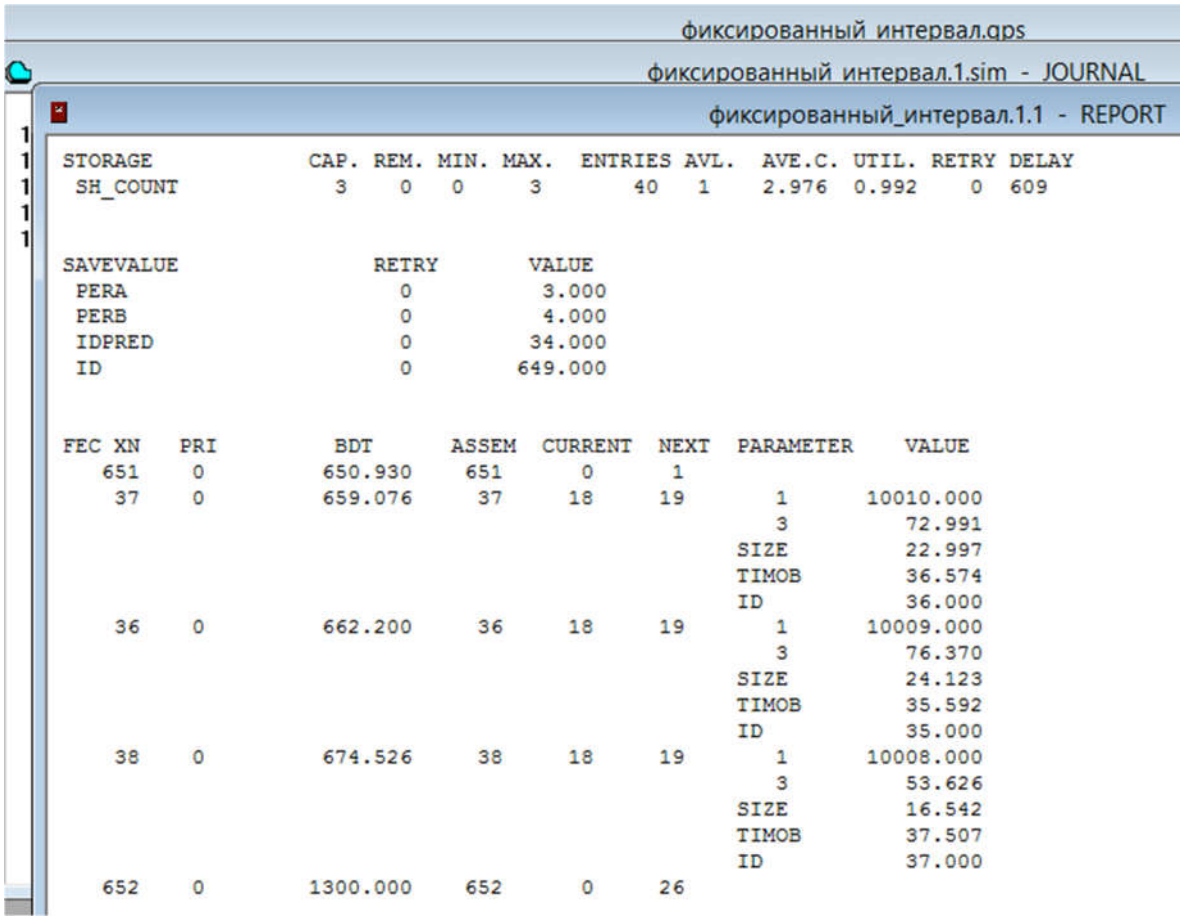
Поток входных данных возможно моделировать несколькими способами, которые по-разному влияют на конечное время обработки пакетов. Выбраны следующие вари-

анты генерации межпакетного интервала: фиксированный межпакетный интервал и случайное распределение интервала следования пакетов.

К примеру, для исследования события поступления пакета на вход скоммутированным устройствам выбрано распределение Пуассона. Поток событий, которые наступают одно за другим в случайные моменты времени, является пуассоновским простейшим, если вероятность появления события K за время T определяется законом Пуассона. Время T между двумя событиями в пуассоновском потоке распределено по экспоненциальному распределению интервалов, соответствующих появлению очередного события [5, 6].

На рис. 3 и 4 представлены фрагменты отчетов при использовании фиксированного межпакетного интервала и интервала, имеющего распределение Пуассона, соответственно.

Особый интерес представляют списки FEC, а именно: столбец XN, отвечающий за номер транзакта. В последней строке столбца XN на рис. 3 находится число 652 – номер последнего транзакта, который пройдет через модель, а на рис. 4 – 648. Следовательно, в случае фиксированного межпакетного интервала за одинаковое время моделирования через блоки модели успевает пройти большее количество транзактов.



фиксированный интервал.gps

фиксированный интервал.1.sim - JOURNAL

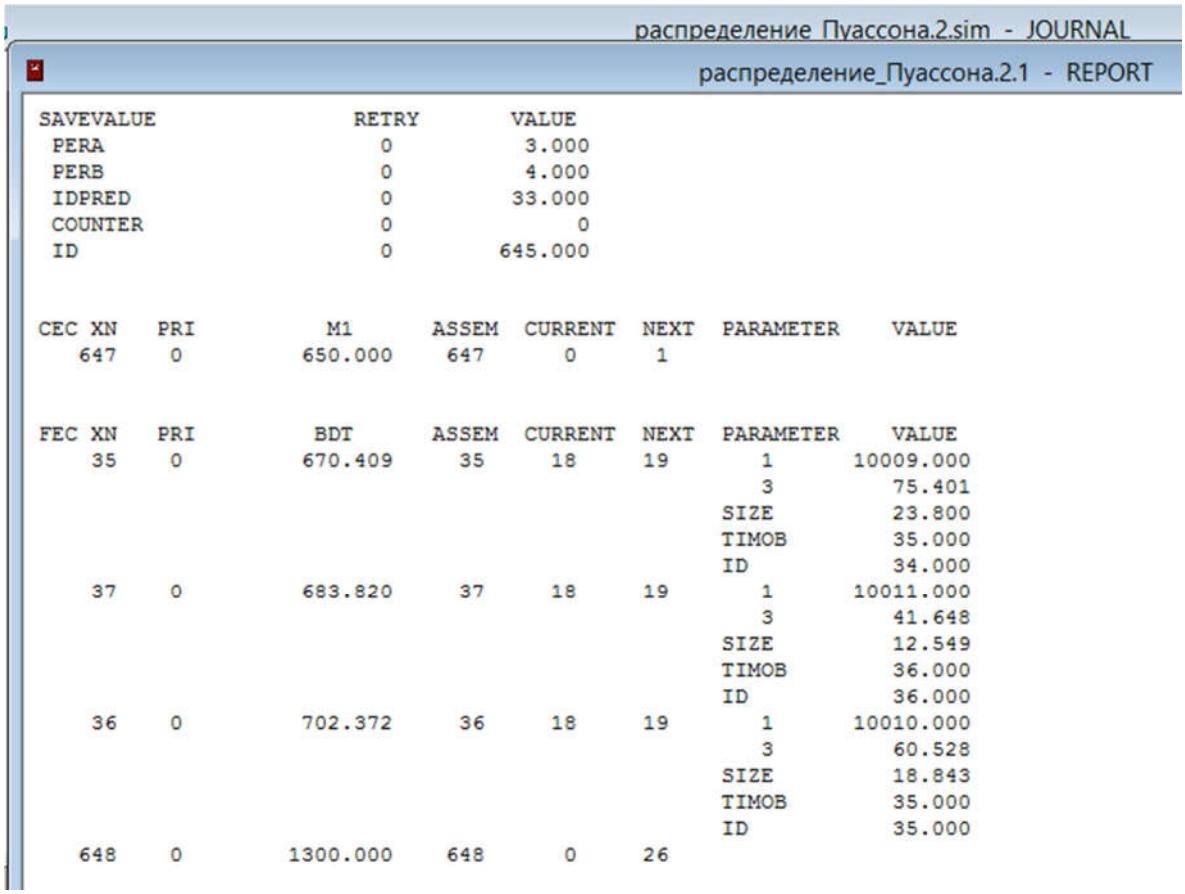
фиксированный_интервал.1.1 - REPORT

STORAGE	CAP.	REM.	MIN.	MAX.	ENTRIES	AVL.	AVE.C.	UTIL.	RETRY	DELAY
SH_COUNT	3	0	0	3	40	1	2.976	0.992	0	609

SAVEVALUE	RETRY	VALUE
PERA	0	3.000
PERB	0	4.000
IDPRED	0	34.000
ID	0	649.000

FEC XN	PRI	BDT	ASSEM	CURRENT	NEXT	PARAMETER	VALUE
651	0	650.930	651	0	1		
37	0	659.076	37	18	19	1	10010.000
						3	72.991
						SIZE	22.997
						TIMOB	36.574
						ID	36.000
36	0	662.200	36	18	19	1	10009.000
						3	76.370
						SIZE	24.123
						TIMOB	35.592
						ID	35.000
38	0	674.526	38	18	19	1	10008.000
						3	53.626
						SIZE	16.542
						TIMOB	37.507
						ID	37.000
652	0	1300.000	652	0	26		

Рис. 3. Использование фиксированного межпакетного интервала при моделировании входного потока



распределение_Пуассона.2.sim - JOURNAL

распределение_Пуассона.2.1 - REPORT

SAVEVALUE	RETRY	VALUE
PERA	0	3.000
PERB	0	4.000
IDPRED	0	33.000
COUNTER	0	0
ID	0	645.000

CEC XN	PRI	M1	ASSEM	CURRENT	NEXT	PARAMETER	VALUE
647	0	650.000	647	0	1		

FEC XN	PRI	BDT	ASSEM	CURRENT	NEXT	PARAMETER	VALUE
35	0	670.409	35	18	19	1	10009.000
						3	75.401
						SIZE	23.800
						TIMOB	35.000
						ID	34.000
37	0	683.820	37	18	19	1	10011.000
						3	41.648
						SIZE	12.549
						TIMOB	36.000
						ID	36.000
36	0	702.372	36	18	19	1	10010.000
						3	60.528
						SIZE	18.843
						TIMOB	35.000
						ID	35.000
648	0	1300.000	648	0	26		

Рис. 4. Использование распределения Пуассона при моделировании входного потока

Однако при рассмотрении сетевого ВШ очевидно, что данные на вход устройства будут поступать неравномерно. В ходе работы исследовано поведение сетевого трафика. Авторами на основе [7] выбрано распределение Гаусса для моделирования ВШ.

Синхронизация работы НШ при параллельном соединении

В ходе изучения основных характеристик модели высокоскоростного шифратора авторами рассмотрены особенности работы устройства ВШ с выходными данными НШ. Также рассмотрена зависимость скорости обработки данных от используемого алгоритма шифрования.

Потоковая скорость обработки данных – это один из основных параметров, по которым оценивают аппаратные шифраторы. Она зависит прежде всего от сложности алгоритма шифрования. Проще всего оценить ее по формуле [1]

$$\upsilon = \frac{w \cdot h}{n}, \tag{1}$$

где w – тактовая частота (10 – 200 Мгц), h – размер стандартного блока шифрования, n – число тактов, требующееся на преобразование стандартного блока.

На данный момент алгоритм «Магма» ГОСТ Р 34.12–2015 [8, 9] достаточно изучен, поэтому все расчеты и моделирование будут производиться для этого алгоритма. По данным [1] алгоритм «Магма» имеет быстродействие n = 32 такта на h = 8 байт, следовательно, к примеру, скорость шифрования должна стремиться к 25 Мбайт/с при тактовой частоте w = 100 МГц.

Для корректной работы ВШ необходимо обеспечить синхронизацию устройств НШ. Поэтому выполнено исследование возможных алгоритмов синхронизации.

Рассмотрим случай нарушения последовательности следования пакетов, представленный на рис. 5, где *№* – номер пакета при поступлении. Время обработки *t1* > *t2*, следовательно, пакет с *№ = n+1* придет на выход раньше.

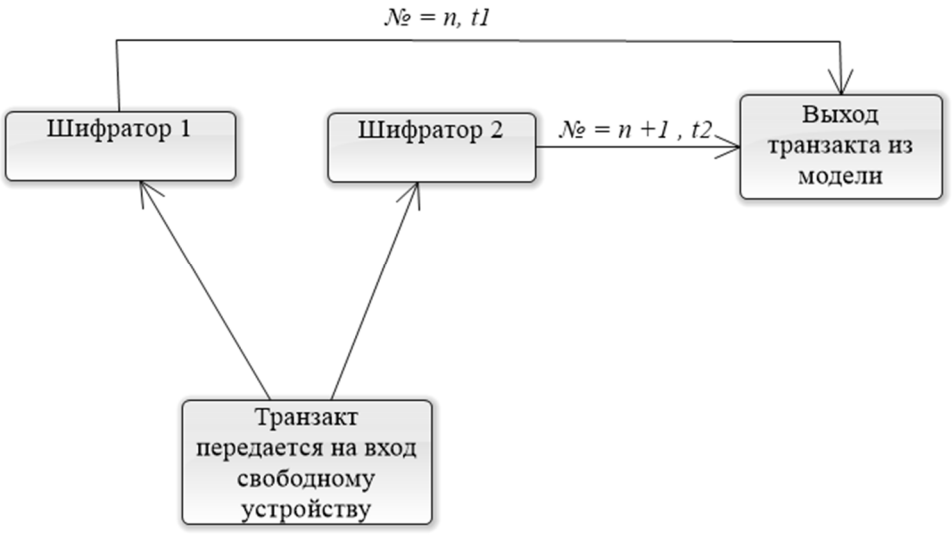


Рис. 5. Схема нарушения синхронизации

Следовательно, необходимо рассмотреть возможность синхронизации процессов устройств по времени.

Задержка выхода пакетов в шифраторе

На рис. 6 представлена общая структура модели ВШ с применением временной задержки для синхронизации следования пакетов.

Рассмотрим используемый в модели способ синхронизации очереди пакетов на выходе модели, представленный на рис. 6 [10]. Пакет передается на обслуживание, в этот момент вычисляется время завершения обслуживания этого пакета (время выхода пакета), которое записывается в сохраняемую величину. Происходит сравнение вычисленного времени с максимальным временем выхода, которое хранится в переменной. Если время завершения обслуживания больше, чем максимальное время, то синхронизация сохранится, максимальному времени обслуживания будет назначено новое значение – время окончания обработки текущего пакета, записанное в сохраняемой переменной, иначе – добавится дополнительная задержка для этого блока. В этом случае будет достигнута синхронизация на выходе, то есть последовательность номеров входящих пакетов будет соответствовать этой же последовательности на выходе. На схеме основных этапов описанного алгоритма синхронизации на рис. 6 $t_{зав}$ – время заверше-

ния обслуживания пакета (транзакта), T_{max} – максимальное время выхода пакета (транзакта).

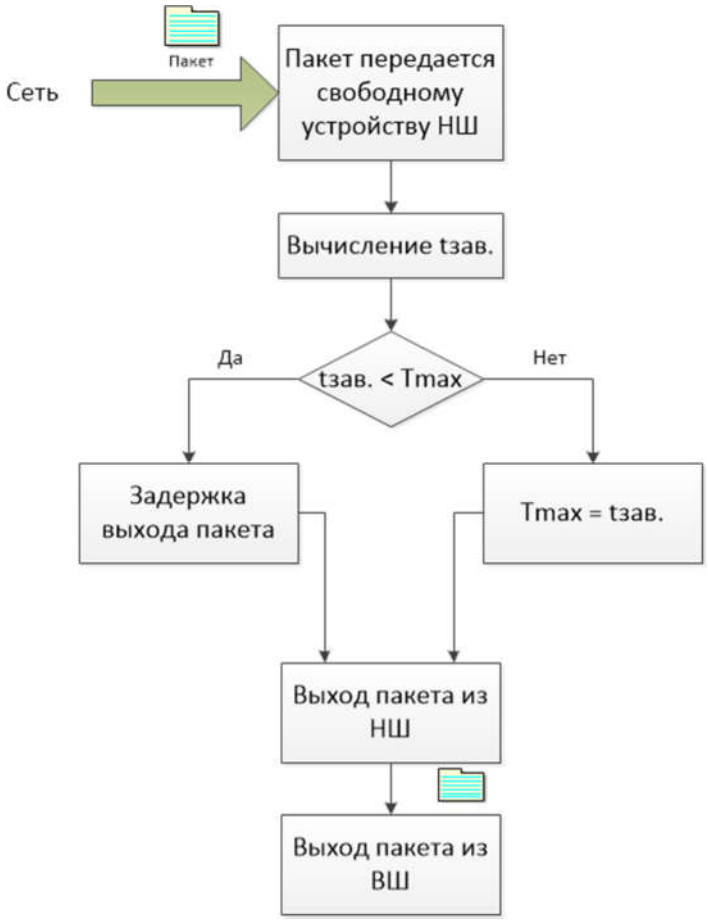


Рис. 6. Структура модели ВШ с задержкой выхода пакетов в шифраторе

Упорядочивающий буфер

В ходе исследования было предложено использование упорядочивающей очереди для синхронизации пакетов на выходе ВШ. Общая схема работы модели, реализующей упорядочивающую очередь, представлена на рис. 7.

Память упорядочивающей очереди. Предполагается, что это энергозависимая память, отдельная микросхема, для которой необходимо оценить объем. Данная часть конечного устройства нужна для того, чтобы задержка, требуемая для синхронизации НШ и правильного порядка пакетов на выходе [10], выполнялась не на устройстве НШ, а в отдельной очереди. Для расчета понадобятся значения параметров формулы

$$T = \frac{l}{\upsilon} + b, \tag{2}$$

где υ – потоковая скорость обработки данных, l – длина пакета, $b = k \cdot \frac{1}{w}$, где k находится в интервале от 40 до 100.

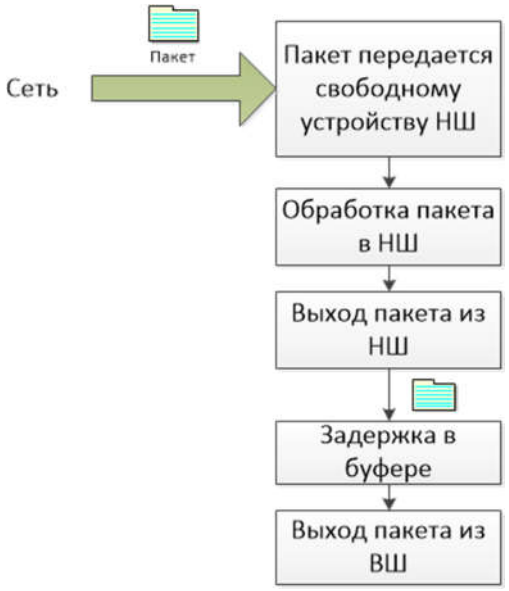


Рис. 7. Структура модели ВШ с упорядочивающим буфером

Для расчета размера упорядочивающего буфера введем следующие обозначения:

$V_{\text{п}}$ – объем памяти, необходимый для хранения одного пакета;

$V_{\text{с}}$ – объем памяти, необходимый для хранения одного символа;

$V_{\text{б}}$ – объем буфера;

$l_{\text{п}}$ – длина пакета;

q – количество пакетов, нуждающихся в синхронизации;

$l_{\text{max/min}}$ – максимальная/минимальная длина пакета рассматриваемого диапазона возможных длин пакетов;

$T_{\text{max/min}}$ – максимальное/минимальное время обработки пакета;

i – счетчик суммирования;

p – вес символа – объем памяти, занимаемый одним символом, зависящий от кодировки и используемого алгоритма шифрования.

Тогда объем памяти для хранения одного пакета рассчитывается по формуле

$$V_{\text{п}} = l_{\text{п}} \cdot V_{\text{с}}. \tag{3}$$

А объем памяти буфера рассчитывается по формуле

$$V_{\text{б}} = \sum_{i=1}^{q} V_n = \sum_{i=1}^{q} l_{\text{п}} \cdot V_{\text{с}}. \tag{4}$$

Предположим, открытый текст находится в кодировке ASCII, в которой один байт содержит один символ, алгоритм шифрования такой, что вес открытого символа равен весу зашифрованного, то есть один символ отрытого текста после применения алгоритма шифрования переходит в один символ зашифрованного текста. Длина пакета генерируется в интервале (l_{min} – l_{max}) символов для конкретного выбранного уровня, используется равномерное распределение [10]. Основной вопрос: каково количество пакетов, которые могут находиться в очереди на синхронизацию одновременно?

Рассмотрим случай: первый пришедший на вход пакет имеет максимальную в пределах рассматриваемого диапазона длину l_{max}, поступает на вход первому шифратору и занимает его на время, рассчитанное по формуле (2), при соответствующих υ и b. Последующие пакеты, которые будут распределены между свободными вторым и третьим шифраторами, будут иметь наименьшую длину рассматриваемого диапазона – l_{min} – и соответствующее время обработки. Таким образом, к моменту освобождения первого шифратора в буфере синхронизации накопятся определенное количество пакетов, ждущие первый. Проведенный ряд подобных вычислений позволяет получить формулу для расчета размера буфера $V_б$:

$$V_б = \frac{T_{max}}{T_{min}} \cdot \left(l_{max} - l_{min}\right) \cdot \frac{p}{2}, \tag{5}$$

где $T_{max/min} = \frac{l_{max/min}}{\upsilon} + b$. Возможно, это не рациональный размер буфера, но такого количества памяти должно хватить на решение поставленной задачи.

Такой подход к синхронизации устройств шифрования поможет прогнозировать нагрузку сети, позволит не занимать ресурсы НШ, а также предотвратит использование скрытых каналов передачи информации благодаря выравниванию трафика на выходе высокоскоростного шифратора.

Анализ отчетов

Авторами разработаны модели ВШ с применением методов синхронизации следования пакетов, рассмотренных в разделе 3: с применением задержки в шифраторе (ВШ_1) и с использованием упорядочивающего буфера (ВШ_2). Анализ отчетов работы полученных моделей рассмотрен на рис. 8 – 11.

LABEL	LOC	BLOCK TYPE	ENTRY COUNT	CURRENT COUNT	RETRY
	1	GENERATE	1	0	0
	2	SAVEVALUE	1	0	0
	3	SAVEVALUE	1	0	0
	4	TERMINATE	1	0	0
	5	GENERATE	822	0	0
	6	SAVEVALUE	822	0	0
	7	ASSIGN	822	0	0
	8	ASSIGN	822	0	0
	9	ASSIGN	822	0	0
	10	ASSIGN	822	0	0
	11	ENTER	822	0	0
	12	TRANSFER	822	0	0
OPR1	13	SEIZE	426	0	0
	14	ASSIGN	426	0	0
	15	TRANSFER	426	0	0
OPR2	16	SEIZE	262	0	0
	17	ASSIGN	262	0	0
	18	TRANSFER	262	0	0
OPR3	19	SEIZE	134	0	0
	20	ASSIGN	134	0	0
COME	21	LEAVE	822	0	0
	22	ADVANCE	822	1	0
	23	ASSIGN	821	0	0
RET	24	TEST	1685	0	0
	25	SAVEVALUE	821	0	0
	26	RELEASE	821	0	0
	27	TERMINATE	821	0	0
LABEL_NEWMAX	28	ADVANCE	864	0	0
	29	TRANSFER	864	0	0
	30	GENERATE	1	0	0
	31	TERMINATE	1	0	0

Рис. 8. Фрагмент отчета ВШ_1 (1)

LABEL	LOC	BLOCK TYPE	ENTRY COUNT	CURRENT COUNT	RETRY
	1	GENERATE	1	0	0
	2	SAVEVALUE	1	0	0
	3	SAVEVALUE	1	0	0
	4	TERMINATE	1	0	0
	5	GENERATE	823	0	0
	6	SAVEVALUE	823	0	0
	7	ASSIGN	823	0	0
	8	ASSIGN	823	0	0
	9	ASSIGN	823	0	0
	10	ASSIGN	823	0	0
	11	ENTER	823	0	0
	12	TRANSFER	823	0	0
OPR1	13	SEIZE	444	0	0
	14	ASSIGN	444	0	0
	15	TRANSFER	444	0	0
OPR2	16	SEIZE	286	0	0
	17	ASSIGN	286	0	0
	18	TRANSFER	286	0	0
OPR3	19	SEIZE	93	0	0
	20	ASSIGN	93	0	0
COME	21	LEAVE	823	0	0
	22	ADVANCE	823	1	0
	23	SAVEVALUE	822	0	0
	24	ASSIGN	822	0	0
	25	RELEASE	822	0	0
	26	QUEUE	822	0	0
	27	SAVEVALUE	822	822	0
	28	TEST	0	0	0
	29	DEPART	0	0	0
	30	SAVEVALUE	0	0	0
	31	TERMINATE	0	0	0
	32	GENERATE	1	0	0
	33	TERMINATE	1	0	0

Рис. 9. Фрагмент отчета ВШ_2 (1)

В представленных на рис. 8 и 9 фрагментах отчетов столбец ENTRY COUNT содержит значения количества транзактов, прошедших через каждый блок за время моделирования. Заметим, наибольшее число транзактов прошло через блоки, относящиеся к метке OPR1, то есть к первому НШ. Это может быть связано с тем, что пакеты поступали на вход настолько неравномерно, что б□льшую их часть успевал обработать OPR1, или таким образом, что первый шифратор получал более короткие пакеты и, следовательно, справлялся с обработкой быстрее других и за время моделирования успел обработать больше пакетов.

Рис. 10 и 11 отображают устройства (FACILITY) и хранилища (STORAGE), присутствующие в модели: FACILITY – список работающих устройств: OP1 – OP3 – первый – третий НШ соответственно; ENTRIES – количество транзактов, прошедших через устройство за время моделирования; UTIL – коэффициент использования оборудования, который показывает, что OP3 (см. рис. 11), к примеру, бездействовал (1 – 0,153) 100 % = 84,7 %, времени работы модели. Анализируя коэффициенты использования оборудования, получаем, что ВШ_2 менее загружен. Параметр AVE.TIME – среднее время обработки одного транзакта устройством, имеет большие значения для модели ВШ_1, это подтверждает большую загруженность этого ВШ.

FACILITY	ENTRIES	UTIL.	AVE. TIME	AVAIL.	OWNER	PEND	INTER	RETRY	DELAY
OP1	426	0.741	50.125	1	824	0	0	0	0
OP2	262	0.519	57.010	1	0	0	0	0	0
OP3	134	0.256	54.946	1	0	0	0	0	0

STORAGE	CAP.	REM.	MIN.	MAX.	ENTRIES	AVL.	AVE.C.	UTIL.	RETRY	DELAY
SH_COUNT	3	3	0	2	822	1	0.004	0.001	0	0

SAVEVALUE	RETRY	VALUE
H	0	64.000
NO	0	32.000
IDPRED	0	821.000
VALUEW	0	353.586
VALUEK	0	55.630
ID	0	822.000

Рис. 10. Фрагмент отчета ВШ_1 (2)

FACILITY	ENTRIES	UTIL.	AVE. TIME	AVAIL.	OWNER	PEND	INTER	RETRY	DELAY
OP1	444	0.716	46.422	1	825	0	0	0	0
OP2	286	0.474	47.692	1	0	0	0	0	0
OP3	93	0.153	47.281	1	0	0	0	0	0

QUEUE	MAX	CONT.	ENTRY	ENTRY(0)	AVE.CONT.	AVE.TIME	AVE.(-0)	RETRY
OCH	822	822	822	0	409.620	14351.652	14351.652	0

STORAGE	CAP.	REM.	MIN.	MAX.	ENTRIES	AVL.	AVE.C.	UTIL.	RETRY	DELAY
SH_COUNT	3	3	0	1	823	1	0.000	0.000	0	0

Рис. 11. Фрагмент отчета ВШ_2 (2)

Полученные результаты позволяют сделать вывод о рекомендованном использовании упорядочивающего буфера для синхронизации устройств НШ. В сравнении с использованием временной задержки для обеспечения синхронизации на выходе пакетов из устройства ВШ использование упорядочивающего буфера повышает производительность устройства ВШ в целом, и, следовательно, качество использования ВШ возрастает.

Заключение

В процессе выполнения работы были получены следующие основные результаты:

– произведен анализ возможных способов построения ВШ;

– определены параметры шифратора, необходимые для моделирования ВШ;

– изучена формула расчета потоковой скорости обработки данных и времени обслуживания транзактов;

– проанализированы способы моделирования входного потока;

– получена формула расчета размера упорядочивающего буфера;

– построена и проанализирована модель, реализующая упорядочивающую очередь для синхронизации устройств НШ;

– создана и проанализирована модель ВШ с использованием полученных значений компонент и выполняющая задержку пакетов в устройстве шифрования для синхронизации следования пакетов.

В дальнейших исследованиях следует изучить характеристики упорядочивающего буфера: сколько максимально/минимально пакетов и при каких условиях могут одновременно находиться в памяти; какой интервал времени в среднем необходим для синхронизации пакетов. В будущих работах планируется детально изучить и, возможно, усовершенствовать полученную в работе формулу (5) расчета размера упорядочивающего буфера.

СПИСОК ЛИТЕРАТУРЫ:

1. Аппаратные шифраторы [Электронный ресурс] / Режим доступа: http://www.osp.ru/pcworld/2002/08/163808/ (дата обращения 25.10.2015).
2. Епишкина, А.В. Кирякина С.А. Имитационное моделирование как инструмент для построения высокоскоростного шифратора // Безопасность информационных технологий. 2015. № 3. С. 44 51.
3. Криптография? Железно! [Электронный ресурс] / Режим доступа: http://www.infosecurity.ru/_gazeta/content/030701/article01.html (дата обращения 25.10.2015).
4. Сетевое шифрование [Электронный ресурс] / Режим доступа: http://ru.thales-esecurity.com/solutions/by-technology-focus/network-encryption (дата обращения 25.10.2015).
5. Система имитационного моделирования GPSS [Электронный ресурс] / Режим доступа: http://gpss-forum.narod.ru/lab4.htm (дата обращения 24.10.2015).
6. Работа с байтами [Электронный ресурс] / Режим доступа: http://mirtelekom.com/gpss3/theory59.htm (дата обращения 20.09.2015).
7. Лукашенко О.В., Морозов Е.В., Пагано М. Применение гауссовских процессов в моделировании сетевого трафика // Труды Карельского научного центра РАН. 2010. № 3. С. 51–58.
8. ГОСТ Р 34.13–2015: стандарт строгого режима [Электронный ресурс] / Режим доступа: http://www.itsec.ru/articles2/crypto/gost-standart-strogogo-rezhima (дата обращения 25.10.2015).
9. ГОСТ Р 34.12–2015. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2015. 25 с.
10. 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». 2015. С. 141–143.

REFERENCES:

1. Apparatnye shifratory [Electronic resource]. – Access mode to the resource: http://www.osp.ru/pcworld/2002/08/163808/ (date of the request 25.10.2015).
2. Epishkina A.V., Kiryakina S.A. Imitacionnoe modelirovanie kak instrument dlya postroeniya vysokoskorostnogo shifratora // Bezopasnost' informacionnyh tekhnologij. 2015. № 3. C. 44 51.
3. Kriptografiya? Zhelezo! [Electronic resource]. – Access mode to the resource: http://www.infosecurity.ru/_gazeta/content/030701/article01.html (date of the request 25.10.2015).
4. Setevoe shifrovanie [Electronic resource]. – Access mode to the resource: http://ru.thales-esecurity.com/solutions/by-technology-focus/network-encryption (date of the request 25.10.2015).
5. Sistema imitacionnogo modelirovaniya GPSS [Electronic resource]. – Access mode to the resource: http://gpss-forum.narod.ru/lab4.htm (date of the request 24.10.2015).
6. Rabota s bajtami [Electronic resource]. – Access mode to the resource: http://mirtelekom.com/gpss3/theory59.htm (date of the request 20.09.2015).
7. Lukashenko O.V., Morozov E.V., Pagano M. Primenenie gaussovskih processov v modelirovanii setevogo trafika // Trudy Karel'skogo nauchnogo centra RAN. 2010. № 3. Pp. 51–58.
8. GOST R 34.13–2015: standart strogogo rezhima [Electronic resource]. – Access mode to the resource: http://www.itsec.ru/articles2/crypto/gost-standart-strogogo-rezhima (date of the request 25.10.2015)
9. GOST R 34.12–2015. Informacionnaya tekhnologiya. Kriptograficheskaya zashchita informacii. Blochnye shifry. M.: Standartinform, 2015. 25 s.
10. Epishkina A.V., Kiryakina S.A. Ob imitacionnom modelirovanii raboty vysokoskorostnogo shifratora // Materialy 24-oj nauchno-tekhnicheskoj konferencii «Metody i tekhnicheskie sredstva obespecheniya bezopasnosti informacii». 2015. S. 141 143.