УДК 681.3

Р. В. Мещеряков, С. К. Росошек, А. А. Шелупанов, М. А. Сонькин

ЗАЩИЩЕННАЯ СЕТЬ ПЕРЕДАЧИ ДАННЫХ НА ОСНОВЕ ПАКЕТНОГО КОНТРОЛЛЕРА

Рассматривается сеть передачи данных в системе с ограниченными ресурсами при распределенной организации обработки информации для различных режимов работы. Приводится сравнительный анализ вычислительной сложности и требуемых объемов памяти.

В настоящее время существует множество различных сетей и систем передачи данных. Тем не менее остаются нерешенными вопросы передачи данных в труднодоступные районы. Очевидно, что имеющиеся решения с использованием современных средств передачи данных в настоящее время достаточно дорогие. Необходимо отметить, что фирмой ООО «Инком» разработан пакетный контроллер «ВИП-М», позволяющий в пакетном режиме передавать цифровую информацию посредством использования существующих сетей передачи данных (рис. 1). Вместе с тем при передаче конфиденциальной информации согласно [1] необходимо проводить криптографические преобразования по ее закрытию. Основные концепции по встраиванию криптографических функций в ВИП изложены в [2].

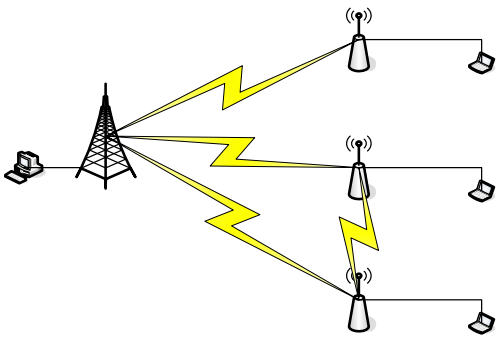

Рис. 1

Криптографическое обеспечение. Согласно действующему законодательству в Российской Федерации допущен к применению только ГОСТ 28147–89. «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» [3]. Размер ключей шифрования составляет 256 бит, блок обработки – 64 бит. Особенностью данного алгоритма является принадлежность к группе симметричных криптографических алгоритмов, что подразумевает наличие одного и того же ключа у абонентов системы.

ГОСТ 28147–89 подразумевает наличие четырех видов использования криптосхемы:

– зашифровывание (расшифровывание) данных в режиме простой замены;

– зашифровывание (расшифровывание) данных в режиме гаммирования;

– зашифровывание (расшифровывание) данных в режиме гаммирования с обратной связью;

– режим выработки имитовставки.

Криптографические преобразования имеют значительную сложность (что при ограниченных вычислительных ресурсах особенно важно), и в целях унификации и обеспечения независимости функции приема/передачи информации целесообразно разнести (рис. 1). Также необходимо обеспечить возможность передачи ключа в криптопроцессор, минуя устройство приема/передачи информации, и через него [2].

Кроме того, использование всех четырех видов криптосхемы в различных комбинациях с дополнительными условиями повышает криптографическую стойкость. Режим выработки имитовставки с некоторыми доработками не только обеспечивает проверку целостности передаваемого сообщения, но и авторство передаваемого сообщения, и отказаться от схемы использования электронно-цифровой подписи согласно ГОСТ 34.10–2001, реализация которого требуют существенно больших вычислительных ресурсов по сравнению с режимом симметричного шифрования, нет необходимости.

Взаимодействие абонентов защищенной сети. В базовой схеме работы пакетного контроллера существуют 2 режима работы:

– связь «точка-точка», позволяющая обеспечивать обмен информацией двух абонентов системы при наличии установившегося канала передачи данных;

– связь «широковещательное оповещение», позволяющая передавать информацию от одного абонента одномоментно нескольким абонентам системы.

В каждом из режимов определен инициатор связи, называемый «Центр и Абонент системы (А)». В зависимости от накладываемых функций на криптопроцессор можно выделить основные технологии его использования. Таким образом, при различных реализациях алгоритмов может быть реализовано несколько режимов работы защищенной сети на основе пакетного контроллера. При этом одним из наиболее важных элементов работы сети является начальный режим работы сети. Необходимо отметить, что режимы работы сети зависят от возможностей криптографического процессора, которые формируют общий ключ симметричного криптографического алгоритма.

Сеанс связи «точка-точка» (рис. 2). Криптопроцессору принадлежит встроенный датчик случайных (псевдослучайных) чисел ДСЧ (ДПСЧ). В Центре имеется библиотека чисел p и α, кото-

Станция Оператор ВИП

рые определяют основные параметры выработки общего ключа (рис. 3). Так как размер библиотеки значительно ограничен, то используется расширение числа p посредством имитовставки: $p' = h(p)$, что позволяет увеличить длину ключа. Затем с помощью ДСЧ (ДСПЧ) выбирает случайное целое число x в интервале $1 < x < p$ и вычисляет $\gamma = \alpha^x \bmod p$. Соответственно для γ также применяется функция имитовставки $\gamma' = h(\gamma)$. Получившаяся тройка $< p', \gamma', \alpha >$ передается по открытому каналу абоненту (рис. 3, направление 1).

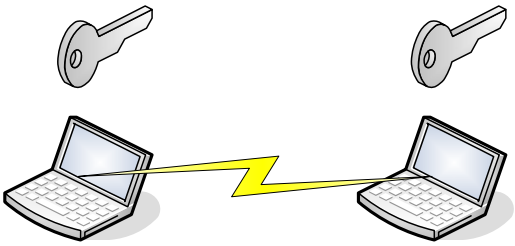

Рис. 2

Рис. 3

Абонент после получения тройки $< p', \gamma', \alpha >$ убирает имитовставки и получает тройку $< p, \gamma, \alpha >$. Затем Абонент выбирает случайное целое y в интервале $1< y < p$, вычисляет $\mu = \alpha^y \bmod p$, делает имитовставку для μ и полученное число μ' отправляет в Центр. Абонент вычисляет общий с Центром ключ $K = \gamma^y \bmod p = \alpha^{xy} \bmod p$ (рис. 3, направление 2). С другой стороны, Центр, получив μ' от Абонента, убирает имитовставку, получает μ и вычисляет общий с Абонентом ключ: $K = \mu^x \bmod p = \alpha^{yx} \bmod p$.

Центр шифрует ключом K соответственно ГОСТ 28147–89 сообщение m и $c = K(m)$ и передает информацию Абоненту (рис. 2, направление 3).

Дальнейшая пересылка может идти в обоих направлениям, так как у Абонента и Центра имеется общий ключ. Получив шифртекст c, Абонент применяет $K(c) = m$.

Таким образом, генерация и использование ключей осуществляется только на период одного сеанса связи. Особые действия при компрометации ключей не требуются – потеря одного аппарата может быть легко блокирована посредством определения его адреса, обязательного к использованию при обмене информацией между абонентами.

Сеанс связи «*широковещательно оповещение*» (рис. 4). Криптопроцессору принадлежит встроенный датчик случайных (псевдослучайных) чисел ДСЧ (ДПСЧ). В Центре, как и в случае с сеансом связи «точка-точка», имеется библиотека чисел p и α, которые определяют основные параметры выработки общего ключа. Затем расширяется число p посредством имитовставки: $p' = h(p)$, что позволяет увеличить длину ключа. Затем с помощью ДСЧ (ДСПЧ) выбирает случайное целое число x в интервале $1 < x < p$ и вычисляет $\gamma = \alpha^x \bmod p$. Соответственно для γ также применяется функция имитовставки $\gamma' = h(\gamma)$. Получившаяся тройка $< p', \gamma', \alpha >$ передается по открытому каналу всем абонентам системы $A_1, A_2, \ldots, A_n$. Каждый из абонентов A_i ($i = 1 \ldots n$) после получения от Центра тройки $< p', \gamma', \alpha >$ убирает имитовставки и получает тройку $< p, \gamma, \alpha >$. Затем каждый Абонент A_i выбирает случайное целое y_i в интервале $1 < y_i < p$, вычисляет $\mu_i = \alpha^{yi} \bmod p$, делает имитовставку для μ_i и полученное число μ_i' отправляет в Центр. Затем каждый Абонента A_i вычисляет общий с Центром ключ $K_i = \gamma^{yi} \bmod p = \alpha^{xyi} \bmod p$.

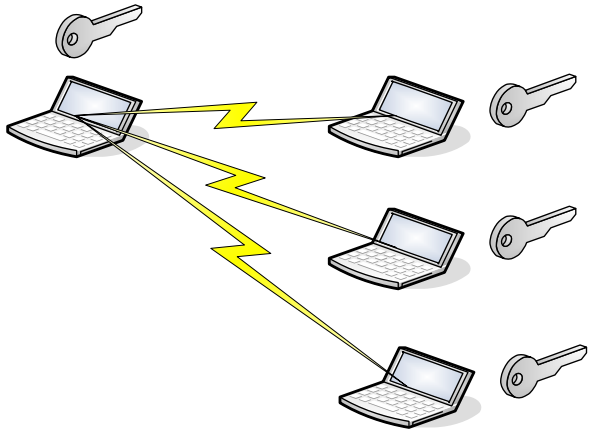

Рис. 4

С другой стороны, Центр, получив от каждого Абонента A_i обратную посылку μ_i', убирает имитовставку и получает набор значением μ_i. Затем для каждого Абонента A_i вычисляет общий с каждым Абонентом ключ: $K_i = \mu_i^x \bmod p = \alpha^{yix} \bmod p$.

После выполнения всех действий по установке общих парных ключей K_i Центр для каждого из Абонентов A_i шифрует сообщение m собственным ключом K_i по ГОСТ 28147–89 и получает n сообщений $c_i = K_i(m)$ и передает Абонентам A_i.

Соответственно, принимая сообщения, Абонент выбирает собственное сообщение c_i и расшифровывает парным ключом K_i путем обратного преобразования $K_i(c_i) = m$.

Таким образом, генерация и использование ключей осуществляет только на период одного сеанса связи. Важное требование: ключ Центра с каждым абонентом системы уникален. Использование одного и того же ключа для связи с различными абонентами существенно уменьшает криптографическую стойкость схемы и она не должна быть использована. Схему, состоящую в том, что на сеансовых ключах передать всем абонентам один ключ шифрования и далее использовать его

для информационного обмена нельзя, либо крайне нежелательно, не применяют. Особых действия при компрометации ключей не требуется, так как *потеря* одного устройства приема/передачи может быть легко блокирована посредством определения его адреса, обязательного к использованию при обмене информацией непосредственно из Центра. Как видно из предложенной схемы, работа в режиме «широковещательного оповещения» может быть сведена к режиму «точка-точка», далее будем рассматривать только эту схему.

Сеанс связи «точка-точка» с использование главного ключа (рис. 5). Криптопроцессор не имеет встроенного датчика случайных (псевдослучайных) чисел ДСЧ (ДПСЧ). Для повышения надежности криптографической схемы, а также уменьшения нагрузки на криптографический процессор пакетного контроллера в некоторых случаях целесообразно исключить датчик случайных (псевдослучайных) чисел из криптографического процессора пакетного контроллера абонента. В этом случае только в Центре имеется ДСЧ (ДПСЧ), с помощью которого до начала информационного обмена на ключевой носитель генерируется Главный Ключ (ГК) $K_{ГК}$. Один экземпляр ГК передается абоненту системы А, другой остается в Центре. Чтобы повысить стойкост ГК, он используется только для передачи сеансового ключа.

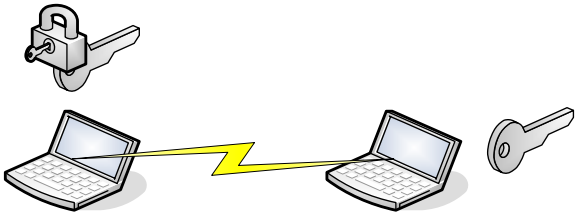

Рис. 5

На первом этапе Центр генерирует сеансовый ключ K_C, шифрует ключ $s = K_{ГК}$ (K_C) (рис. 6), затем посредством имитовставки получает сообщение s' (рис. 6, направление 1). Абонент, получив от Центра сообщение s', убирает имитовставку, расшифровывает сообщение, являющееся сеансовым ключом, $K_C = K_{ГК}$ (s). Используя сеансовый ключ K_C, абонент шифрует сообщение m, получает соответствующее ему зашифрованное сообщение $c = K_C$ (m) и передает в Центр (рис. 6. направление 2). Центр, получив шифрованное сообщение c применяет $m = K_C$ (c), тем самым приобретая исходное сообщение m.

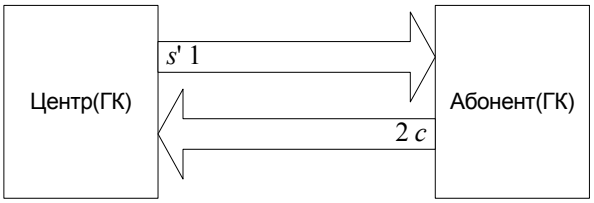

Рис. 6

В случае компрометации ключа требуется смена Главного Ключа, ключи считаются скомпрометированными и использованию более не подлежат. Ключевой носитель может иметь несколько ГК. Различные гК могут располагаться на нескольких ключевых носителях и использоваться в различных режимах работы криптопроцессора.

Сеанс связи «точка-точка» с использованием одноразового блокнота (рис. 7). Криптопроцессор не имеет встроенного датчика случайных (псевдослучайных) чисел ДСЧ (ДПСЧ). Можно несколько упростить предыдущую схему, уменьшив количество генераций случайных (псевдослучайных) последовательностей путем использования схемы «одноразовый блокнот». Так, в Центре имеется ДСЧ (ДПСЧ), с помощью которого до начала информационного обмена на ключевой носитель генерируется Гамма шифра (Г). Один экземпляр Гаммы шифра передается абоненту системы, другой остается в Центре в виде блокнота U. Для повышения стойкости Гамма шифр Г используется исключительно для передачи сеансового ключа и его параметров.

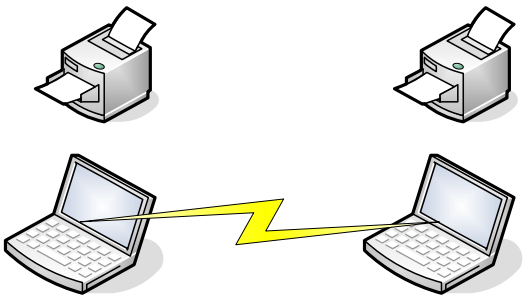

Рис. 7

Таким образом, опишем последовательность установки общего ключа: Центр генерирует сеансовый ключ K_C и режим гаммирования R, затем применяет по режиму R гаммирование (например, функцию «исключающего или», XOR), $s = K_C \oplus Г®$, посредством имитовставки получает сообщение s', Центр передает $< s', R >$ абоненту системы (рис. 8, направление 1).

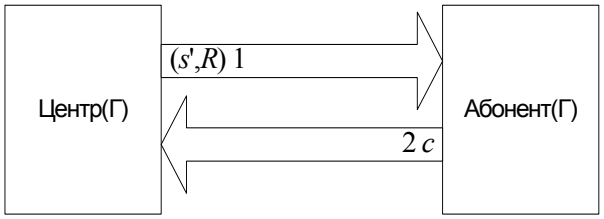

Рис. 8

Абонент, получив пару сообщений $< s', R >$ убирает имитовставку, применяет функцию, обратную гаммированию $K_C = s \oplus Г®$, и сообщение, являющееся сеансовым ключом. Используя сеансовый ключ K_C, абонент шифрует сообщение m и $c = K_C$ (m) и передает в Центр. На последнем этапе Центр получает шифртекст c и применяет $m = K_C ©$.

В случае компрометации ключевого носителя, хранящего Гамму, Гаммы заменяют. Ключевой носитель может иметь любое количество сколько

угодно больших Гамм (единственным ограничением является объем имеющейся памяти) и множество режимов гаммирования, что существенно повышает стойкость.

В случаях, описанных выше Центр должен иметь программное и аппаратное обеспечение для генерации Главного Ключа и Гаммы соответственно. Для хранения ключей допускается применять ПЭВМ Центра, а для криптопреобразований – криптопроцессор.

Расчет нагрузки узлов сети. При учете значительных ограничений на ресурсы криптографического процессора необходимо оценить вычислительные затраты и требуемые объемы памяти для реализации криптографических преобразований.

Оценка вычислительных затрат. Затраты в схеме 1 для Центра и Абонента будут одинаковыми. Учитывая возможности используемого процессора, можем принять следующее:

$$Z = K_s B + K_v \sqrt{B} + K_i B ,$$

где Z – вычислительные затраты; B – длина ключа в битах; K_s – коэффициент, определяющий вычислительные затраты генерации случайного (псевдослучайного числа); K_v – коэффициент, измеряющий вычислительные затраты возведения в степень и взятие по модулю числа; K_i – коэффициент, устанавливающий вычислительные затраты на операцию имитовставки.

Необходимо отметить, что размерность ключа в битах не всегда соответствует максимально допустимой размерности криптографического процессора для выполнения операций за одну команду. В случае если ключ должен быть разбит на K блоков, то длину ключа в битах необходимо считать как $B' = 2^K B$.

Для схемы 2 отличительной особенностью является то, что Центр будет производить затрат в n раз больше, чем в схеме 1.

Для заданной величины битности Центра и Абонента используемого процессора, получены значения в относительных единицах (рис. 9).

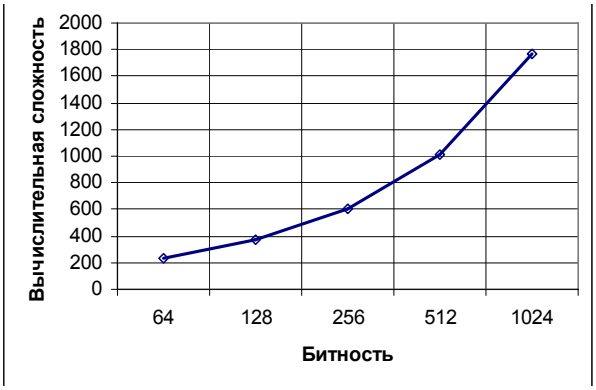

Рис. 9

Для схемы 3 Центра формула упростится:

$$Z = K_s B + K_i B + K_c B ,$$

где Z – вычислительные затраты; B – длина ключа в битах; K_s – коэффициент, измеряющий вычислительные затраты генерации случайного (псевдослучайного числа); K_i – коэффициент, определяющий вычислительные затраты на операцию имитовставки; K_c – коэффициент, устанавливающий вычислительные затраты на шифрование сеансового ключа.

Для криптографического процессора, работающего по схемам 2 и 3 (рис. 10), приведены значения вычислительной сложности в относительных единицах для Центра и Абонента системы. Значения коэффициентов для расчета приняты одинаковыми с вариантом расчета схемы 1.

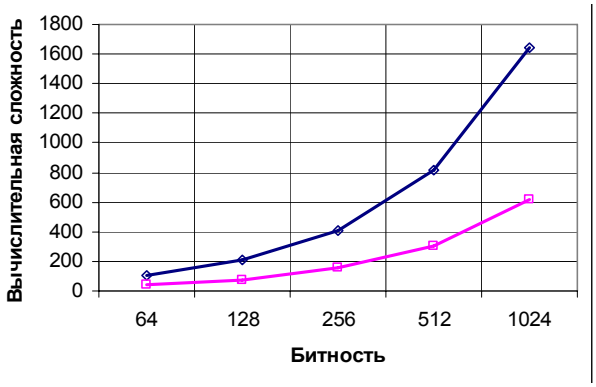

Рис. 10

Необходимо отметить, рост функции для схемы 3 происходит быстрее, чем для схемы 2, учитывая, что процессоры с битностью более 256 имеют большую стоимость. Для Абонента системы вычислительная сложность установки общего ключа примет вид $Z = K_i B + K_c B$.

Для схемы 4 вычислительная сложность будет рассчитываться по выражению

$$Z = K_s B + K_i B + K_\Gamma B ,$$

где Z – вычислительные затраты; B – длина ключа в битах; K_s – коэффициент, измеряющий вычислительные затраты генерации случайного (псевдослучайного числа); K_i – коэффициент, определяющий вычислительные затраты на операцию имитовставки; K_Γ – коэффициент, устанавливающий вычислительные затраты на гаммирование.

Общая функциональная зависимость будет подобна режиму 3.

Необходимо отметить, что после установления общего парного ключа Центра и Абонента системы вычислительная сложность операций шифрования и расшифрования сообщений будет зависеть от реализации ГОСТ 28147–89 [3]. Можно однозначно сказать, что скорость операций шифрования и расшифрования сообщений менее скорости установки общего ключа.

Оценка требуемых объемов памяти. Для хранения ключевой информации и параметров ее получения необходима долговременная память, для вычислимых действий – оперативная память. Объемы требуемой памяти в зависимости от битности параметров и передаваемых сообщений приведены в таблице:

Память для хранения	Схема 1		Схема 2		Схема 3		Схема 4	
	Центр	Абонент	Центр	Абонент	Центр	Абонент	Центр	Абонент
Ключа	$2B$	$2B$	$2B$	$2B$	B	B	UB	UB
Имитовставки или гаммы шифра	hB	hB	hB	hB	hB	hB	$ГВ$	$ГВ$
Оперативной информации для установления общего ключа	$7B+3(1+h)B$	$7B+3(1+h)B$	$(n+1)(7B+3(1+h)B)$	$7B+3(1+h)B$	$2B+(1+h)B$	$2B+(1+h)B$	$2B+(1+h)B$	$2B+(1+h)B$
Передаваемые сообщения для установления общего ключа	$B+2(1+h)B$	$B+2(1+h)B$	$B+2(1+h)B$	$B+2(1+h)B$	$(1+h)B$	0	$B+(1+h)B$	0
Передачи сообщений	lB	lB	lB	lB	lB	lB	lB	lB

Примечание: B – битность ключа, h и $Г$ – коэффициенты увеличения ключа (имитовставки и Гаммы соответственно), U – коэффициент хранения одноразового блокнота, l – величина передаваемого сообщения.

Необходимо отметить, что в данном случае приведены базовые значения. В случае если процессор не имеет возможности работать с данными размерностью B и $(1 + h)B$, то необходимо увеличивать требуемую размерность оперативной памяти в $(K–1)$ раз, где K – количество делений обрабатываемых блоков информации.

С другой стороны, в приведенной таблице выделяются действия только для установления общего ключа. Размерность для проведения операций шифрования и расшифрования при реализации ГОСТ 28147–89 [3] жестко регламентирована и может быть незначительно оптимизирована, поэтому в данной работе этот вопрос не отражен.

Таким образом, В ходе проведения работы были получены результаты по реализации криптографических функций в системах с ограниченными параметрами. Проведен детальный анализ схем установления общего ключа. Рассчитаны оценочные значения требуемых вычислительных ресурсов, а также требуемой памяти для хранения информации.

Библиографический список

1. Основы информационной безопасности / Е. Б. Белов, В. П. Лось, Ф. В. Мещеряков и др. М. : Горячая линия – Телеком, 2006. 544 с.

2. Встраивание криптографических функций в систему связи с ограниченными ресурсами Р. В. Мещеряков, А. А. Шелупанов, С. К. Росошек, С. С. Бондарчук // Вопросы защиты информации. 2004. № 2. С. 22–25.

3. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М. : Изд-во стандартов, 1989.

R. V. Mescheriakov, S. K. Rososhek, A. A. Shelupanov

THE PROTECTED DATA TRANSMISSION NETWORK ON THE MESSAGE CONTROLLER BASIS

It is covered a data transmission network in system with the limited resources at the distributed organization of information processing for various operating modes. It is carried out comparative analysis of a computing complexity and demanded memory sizes.