УДК 004.056.5

С.Н. Новиков
(Сибирский государственный университет телекоммуникаций и информатики;
e-mail: snovikov@mbit.ru)

ОСНОВЫ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ ЗАЩИТЫ ПОЛЬЗОВАТЕЛЬСКОЙ ИНФОРМАЦИИ В МУЛЬТИСЕРВИСНЫХ СЕТЯХ СВЯЗИ

Проведён анализ возможностей использования ресурсов мультисервисных сетей связи для защиты пользовательской информации.

Ключевые слова: мультисервисная сеть, конфиденциальность, целостность, доступность.

S.N. Novikov

THE BASICS OF ENSURING COMPLEX PROTECTION OF USER INFORMATION IN MULTISERVICE NETWORKS CONNECTION

The analysis of possibility use resources of multi-service networks for protection of user information.

Key words: multi-service network, confidentiality, integrity, availability.

Введение

Комплексная защита пользовательской информации является одним из определяющих факторов функционирования ***мультисервисной сети связи (МСС)***, ориентированной на предоставление пользователям неограниченного спектра приложений ***с гарантированным качеством обслуживания*** (англ. Quality of Service, ***QoS***). Проведем анализ известных подходов, обеспечивающих базовые параметры комплексной защиты пользовательской информации [1] (конфиденциальность, целостность и доступность), применительно к требованиям МСС.

Анализ основных подходов по обеспечению конфиденциальности пользовательской информации

Методы обеспечения конфиденциальности основываются на криптографии [2] – шифрование с одним ключом и шифрование с двумя ключами. В первом случае, как правило, время шифрования/расшифрования прямо пропорционально длине ключа и сложности алгоритмов. Недостатком данного подхода является наличие закрытого канала связи для доставки пользователям секретного ключа.

В криптосистемах с двумя ключами данный недостаток отсутствует. Однако зависимость времени шифрования от длины ключа L_k имеет нелинейный характер [3] и в общем случае определяется:

$$t_{\text{ш}} = AL_k^r + B, \qquad (1)$$

где $t_{\text{ш}}$ – время шифрования;

A, B, r – постоянные, значения которых определяются криптографическими алгоритмами.

При больших значениях L_k время шифрования резко возрастает, что является неприемлемым для высокоскоростных приложений, функционирующих в реальном масштабе времени. Поэтому на практике применяют "гибридную" систему шифрования. Асимметричные алгоритмы используются для организации закрытого канала связи, а симметричные алгоритмы – непосредственно для шифрования данных между пользователями.

У данного подхода есть недостаток. Пользователи должны обладать знаниями в области ***защиты информации (ЗИ)*** и иметь дополнительное криптографическое обеспечение, применение которого может быть ограничено вследствие финансовых, технологических или иных затрат.

В работах [4, 5] предложен подход, обеспечивающий конфиденциальность за счёт многопутёвой маршрутизации. Основная идея состоит в разделении сообщения *M* на *n* частей по секретной схеме и последующей отправкой этих частей по *n* независимым маршрутам между ***узлом-источником (УИ)*** и ***узлом-получателем (УП)*** сообщения. Таким образом, если даже какое-то количество маршрутов будет скомпрометировано, то секретное сообщение не будет рассекречено и по *K* доставленным получателю частям будет восстановлено. При этом используется (*K*, *n*) – схема разделения секрета Шамира.

Алгоритм следующий. Выбирается некоторое простое число $p > M$. Формируется многочлен степени $(K - 1)$:

$$F(x) = \left(a_{K-1}x^{K-1} + a_{k-2}x^{K-2} + \ldots + a_1 x + M\right) \bmod p, \qquad (2)$$

где $K \le n$ – ожидаемое минимальное количество частей секретного сообщения *M*, которые будут приняты по независимым маршрутам в УП;

a_{K-1}, a_{k-2}, …, a_1 – некоторые случайные числа.

Вычисляется *n* секретных сообщений:

$$k_i = F(i) = \left(a_{K-1}i^{K-1} + a_{K-2}i^{K-2} + \ldots + a_1 i + M\right) \bmod p; \; i = \overline{1,n},$$

которые вместе с *K* и *p* будут переданы по *n* независимым маршрутам.

В УП принятые *K*, *p* и части секретного сообщения k_i; $i = \overline{1,n}$ позволяют полностью восстановить исходный многочлен (2) (в том числе и исходное сообщение *M*) путём решения системы из $K \le n$ уравнений.

В результате обеспечивается конфиденциальность и QoS приложений пользователя. Кроме того, пользователи не обязаны иметь криптографическое обеспечение и обладать определенными знаниями в области ЗИ.

Однако для реализации данного подхода на сети необходимо организовать минимум три независимых маршрута между УИ и УП с одинаковыми ***вероятностно-временными характеристиками (ВВХ)*** (скорость передачи информации, время задержки, временной джиттер, вероятность ошибочного приема на пакет, символ и так далее). В противном случае передаваемое сообщение в точке приема не будет восстановлено либо будет восстановлено с задержкой во времени, что является критичным для высокоскоростных приложений, функционирующих в реальном масштабе времени.

В работе [6] показано, что многократное "вложение" ассиметричных криптографических алгоритмов существенно сокращает время шифрования при сохранении требуемого уровня конфиденциальности информации.

Пусть l – количество "вложенных" ассиметричных алгоритмов. Введём соответствующие обозначения зашифрования и расшифрования:

$$y = E_{k_l}\left\{...E_{k_i}[...E_{k_1}(x)]\right\}, \quad x = D_{k_1}\left\{...D_{k_i}[...D_{k_l}(y)]\right\}. \qquad (3)$$

Общая длина составного ключа определяется выражением

$$L_{k_{\text{сост}}} = \sum_{i=1}^{l} L_{k_i}.$$

Время задержки при этом сокращается (рис. 1).

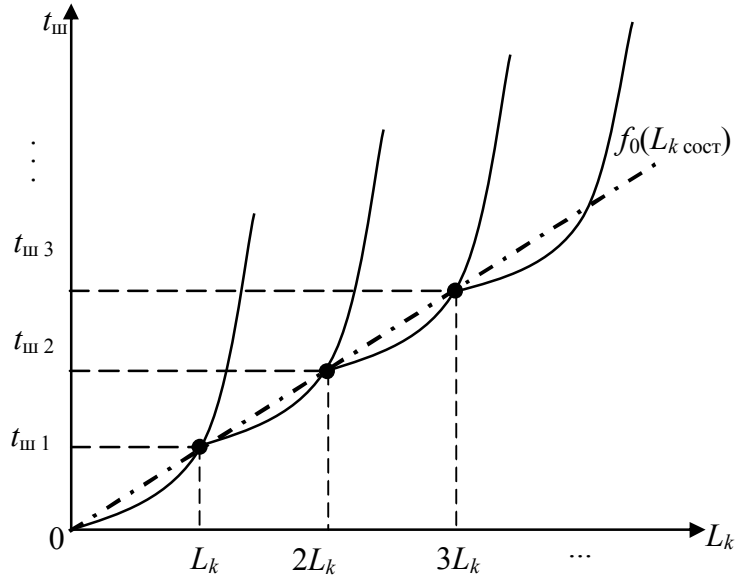

Рис. 1. Зависимости времени, затрачиваемого на шифрование, от длины составного ключа

График зависимости $t_{\text{ш}} = f(L_{k\text{сост}})$ имеет сложную кривую, состоящую из отрезков $t_{\text{ш}} = f(L_{k1}), \ldots, t_{\text{ш}} = f(L_{ki}), \ldots, t_{\text{ш}} = f(L_{kl})$. Для определения общего времени на шифрование $t_{\text{шсост}}$ заменим $t_{\text{ш}} = f(L_{k\text{сост}})$ на линейную $f_0(L_{k\text{сост}})$, так как соответствующие первые производные равны.

Учитывая (1) и характер $f_0(L_{k\text{сост}})$, получим следующий временной выигрыш при шифровании составным ключом (пусть $L_{k_i} = \text{const};\ B = 0$):

$$\frac{t_{\text{ш}}}{t_{\text{шсост}}} = \frac{AL_{k\text{сост}}^r + B}{l\left(A\left(\frac{L_{k\text{сост}}}{l}\right)^r + B\right)} = \frac{AL_{k\text{сост}}^r + B}{lA\left(\frac{L_{k\text{сост}}}{l}\right)^r + lB} = \frac{AL_{k\text{сост}}^r}{lA\left(\frac{L_{k\text{сост}}}{l}\right)^r} = l^{r-1}, \qquad (4)$$

где $t_{\text{ш сост}}$ – время, отводимое на процедуру шифрования алгоритмом, состоящим из нескольких однотипных алгоритмов.

Результаты эксперимента шифрования алгоритмом RSA блока данных 1 *Кбайт* при изменении длины ключа от 256 *бит* до 2048 *бит* и использовании составного 256-битного ключа подтвердили предположение (4).

Сравнительный анализ основных подходов, обеспечивающих конфиденциальность пользовательской информации, приведен в табл. 1.

Таблица 1

Анализ основных подходов, обеспечивающих конфиденциальность информации

№	Способ обеспечения конфиденциальности	Достоинства	Недостатки	
1	Симметричная система шифрования	Высокая скорость шифрования $t_{ш} = AL_k + B$	Наличие закрытого канала связи	Пользователи должны обладать знаниями в области ЗИ и иметь дополнительное специальное криптографическое программно-аппаратное обеспечение
2	Ассиметричная система шифрования	Отсутствие закрытого канала связи	Низкая скорость шифрования $t_{ш} = AL_k^r + B$	
3	"Гибридная" система шифрования	QoS. Отсутствие закрытого канала связи. Высокая скорость шифрования $t_{ш} = AL_k + B$		
4	Многопутевая маршрутизация	QoS. Пользователи не должны обладать знаниями в области ЗИ и иметь криптографическое обеспечение.	Реализация минимум трех независимых маршрутов между УИ и УП с одинаковыми ВВХ	
5	Многократное "вложение" ассиметричных алгоритмов шифрования	QoS. Высокая скорость шифрования $t_{ш} = A\frac{L_{k\text{сост}}^r}{l^{(r-1)}} + Bl$ Отсутствие закрытого канала связи. Пользователи не должны обладать знаниями в области ЗИ и иметь дополнительное криптографическое обеспечение.		

Анализ основных подходов по обеспечению целостности пользовательской информации

На рис. 2 приведены основные подходы, обеспечивающие целостность информации.

Рис. 2. Основные методы, обеспечивающие целостность информации в ТКС

Криптографический метод (хеширование, шифрование, электронная цифровая подпись) [2] подразумевает введение в передаваемое сообщение проверочной комбинации, которая вычисляется по определенным алгоритмам и является "индикатором" нарушения целостности информации. Таким образом, криптографический метод только контролирует целостность информации. В случае её модификации между удаленными пользователями необходимо организовать канал обратной связи [7] и повторную передачу сообщения, то есть выполнить многократное дублирование информации, что значительно влияет на время задержки. В результате, применение в МСС криптографического метода с дублированием информации для обеспечения целостности ограниченно для высокоскоростных приложений, функционирующих в реальном масштабе времени.

Метод резервирования информации подразумевает параллельную передачу информации по n маршрутам и принятие решения о целостности пользовательской информации на приемной стороне [8].

Пусть передаются сообщения $S = \{S_1, S_2\}$ с соответствующими априорными вероятностями $0 \le P(S_i) \le 1$, $\sum_{i=1}^{2} P(S_i) = 1$ (рис. 3). На каждом *i*-м маршруте ($i = \overline{1,n}$) сообщения $S = \{S_1, S_2\}$ модифицируются с вероятностью $P_{\text{м}}^{(i)}$; $i = \overline{1,n}$. Тогда задача обеспечения целостности $S = \{S_1, S_2\}$ сводится к процессу принятия решения ***решающим устройством (РУ)*** в УП по *n* одновременно принятым сообщениям $x = (x_1, ..., x_i, ..., x_n)$.

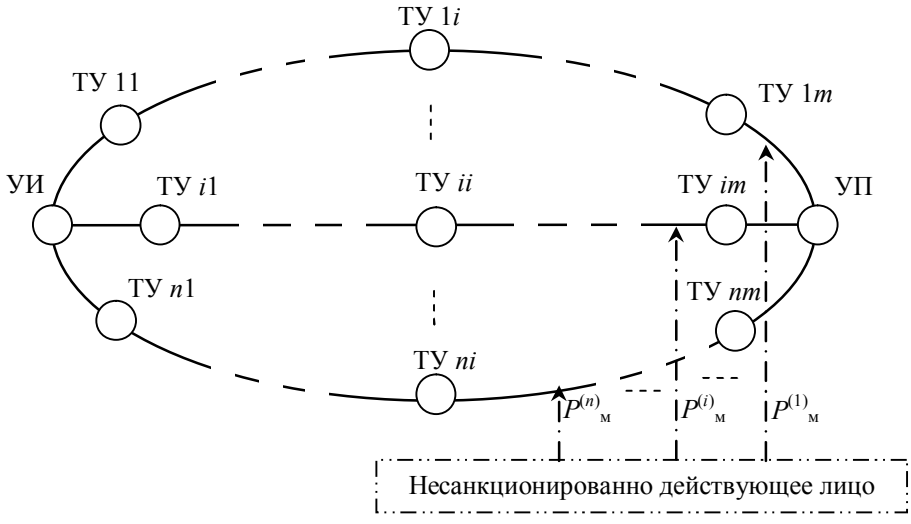

Рис. 3. Структура организации параллельных соединений

Условные вероятности, что на выходе РУ будет S_1 или S_2 определяются:

$$P\left(S_1/\left(x_i;\, i=\overline{0,n}\right)\right)=\frac{P(S_1)\left\{\prod\limits_{i\in x_i=S_1}\left(1-P_{\text{м}}^{(i)}\right)\prod\limits_{i\in x_i=S_2}P_{\text{м}}^{(i)}\right\}}{P\left(x_i;i=\overline{0,n}\right)},$$

$$P\left(S_2/\left(x_i;\, i=\overline{0,n}\right)\right)=\frac{P(S_2)\left\{\prod\limits_{i\in x_i=S_1}P_{\text{м}}^{(i)}\prod\limits_{i\in x_i=S_2}\left(1-P_{\text{м}}^{(i)}\right)\right\}}{P\left(x_i;i=\overline{0,n}\right)}.$$

Возьмем отношение этих выражений. Если полученный результат окажется больше 1, то решение будет принято в пользу S_1, иначе – S_2:

$$\frac{P\left\{S_1/\left(x_i;\ i=\overline{0,n}\right)\right\}}{P\left\{S_2/\left(x_i;\ i=\overline{0,n}\right)\right\}}=\frac{P(S_1)}{P(S_2)}\times\frac{\prod\limits_{i\in x_i=S_1}\left(1-P_{\text{м}}^{(i)}\right)}{\prod\limits_{i\in x_i=S_1}P_{\text{м}}^{(i)}}\times\frac{\prod\limits_{i\in x_i=S_2}P_{\text{м}}^{(i)}}{\prod\limits_{i\in x_i=S_2}\left(1-P_{\text{м}}^{(i)}\right)}. \qquad (5)$$

Прологарифмируем обе части выражения (5):

$$\ln\frac{P\left\{S_1/\left(x_i;\, i=\overline{0,n}\right)\right\}}{P\left\{S_2/\left(x_i;\, i=\overline{0,n}\right)\right\}}=\ln\frac{P(S_1)}{P(S_2)}+\sum_{i\in x_i=S_1}\ln\frac{\left(1-P_{\text{м}}^{(i)}\right)}{P_{\text{м}}^{(i)}}+\sum_{i\in x_i=S_2}\ln\frac{P_{\text{м}}^{(i)}}{\left(1-P_{\text{м}}^{(i)}\right)}. \qquad (6)$$

Введем обозначения:

$$a_0=\ln\frac{P(S_1)}{P(S_2)},\ a_i=\ln\frac{\left(1-P_{\text{м}}^{(i)}\right)}{P_{\text{м}}^{(i)}}. \qquad (7)$$

Пусть условно $S_1=+1,\ S_2=-1$. В результате получим

$$\ln\frac{P\left\{S_1/\left(x_i;\, i=\overline{0,n}\right)\right\}}{P\left\{S_2/\left(x_i;\, i=\overline{0,n}\right)\right\}}=a_0+\sum_{i=1}^{n}a_i x_i. \qquad (8)$$

В результате имеем следующее правило принятия решения:

$$a_0+\sum_{i=1}^{n}x_i a_i=\begin{cases}>0, \text{то}\quad S^*=S_1;\\ <0, \text{то}\quad S^*=S_2.\end{cases} \qquad (9)$$

Функциональная схема РУ представлена на рис. 4.

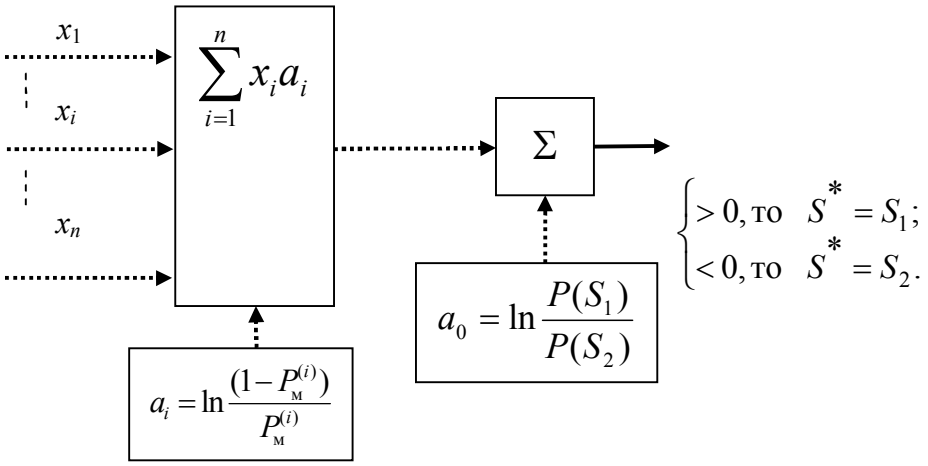

Рис. 4. Функциональная схема РУ

Если вероятности модификации символа по всем маршрутам равны, то есть $P_{\text{м}} = P_{\text{м}}^{(i)}$, а атаки злоумышленных лиц являются независимыми, то вероятность целостности информации на выходе РУ определяется

$$P_{\text{ц РУ}} = 1 - \sum_{i=0}^{\frac{n-1}{2}} \frac{(n-1)...(n-2i+1)}{(n+2i+1)!} (1-P_{\text{м}})^{\frac{n-1-2i}{2}} P_{\text{м}}^{\frac{n+1+2i}{2}}. \qquad (10)$$

Результаты имитационного моделирования функционирования РУ приведены на рис. 5. Моделирование исходящего потока сообщений $S = \{S_1, S_2\}$ из УИ осуществлялось по правилу:

$$S = \begin{cases} S_i = +1, & \text{если} \quad z \le P(S_1); \\ S_i = -1, & \text{если} \quad z > P(S_1). \end{cases}$$

где z – случайное число, генерируемое датчиком случайных чисел с равномерным законом распределения ($0 \le z \le 1$);

$i = \overline{1, N}$;

N – количество сообщений $S = \{S_1, S_2\}$ за период моделирования (количество испытаний).

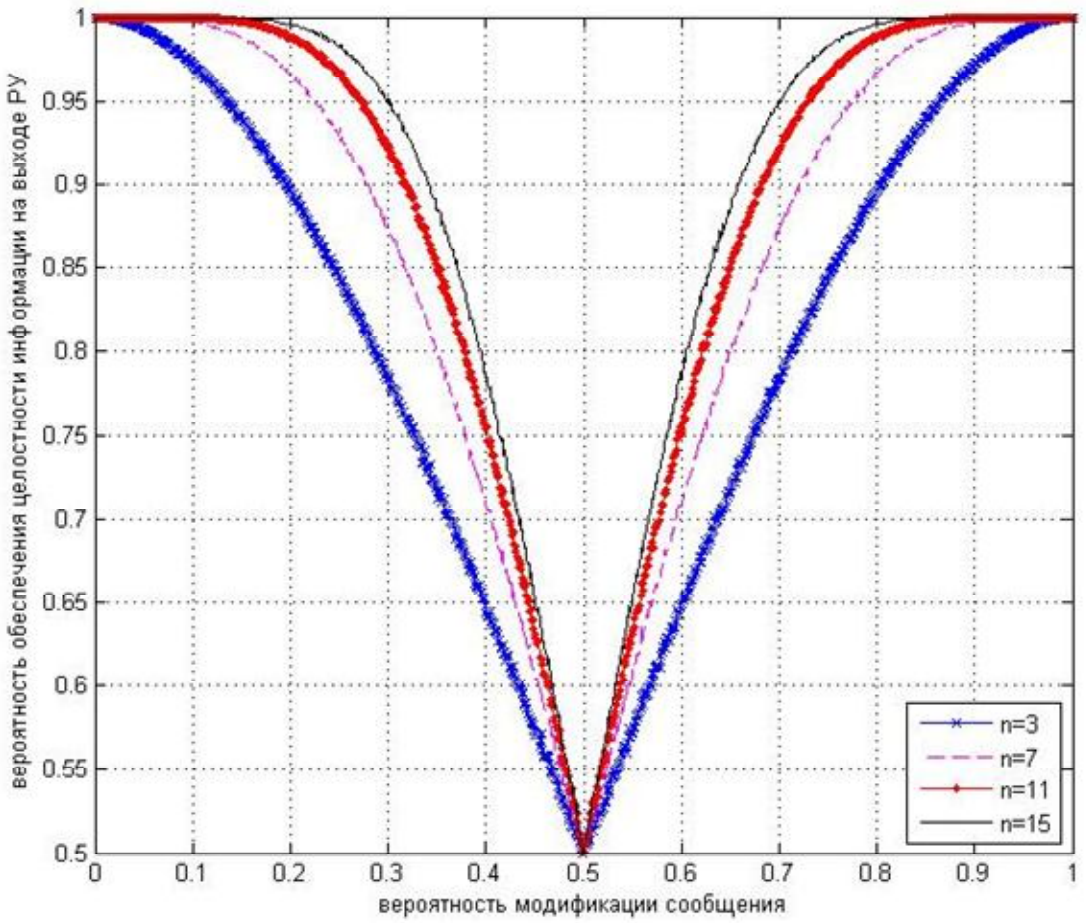

Рис. 5. Семейство графиков зависимости $P_{\text{ц РУ}} = f(P_{\text{м}})$ при разных n

Моделирование модификации каждого из N сообщений $S = \{S_1, S_2\}$ в $i = \overline{1,n}$ независимых соединениях (рис. 3) выполнялось по правилу:

$$x_i = \begin{cases} \text{если } z \le P_{\text{м}}, \text{ то модификация сообщения } S_i \text{ есть, } x_i = S_i \times (-1); \\ \text{если } z > P_{\text{м}}, \text{ то модификации сообщения } S_i \text{ нет, } x_i = S_i, \end{cases}$$

где z – случайное число, генерируемое датчиком случайных чисел с равномерным законом распределения ($0 \le z \le 1$);

$i = \overline{1,n}$.

Зависимости $P_{\text{ц РУ}} = f(P_{\text{м}}, n)$ получены при $N = 30000$ и достоверности $\alpha = 0{,}999$, что обеспечивает абсолютную погрешность результатов моделирования не ниже 1 %.

Анализ основных подходов по обеспечению доступности пользовательской информации

Базовым методом обеспечения доступности информации является резервирование и дублирование как самих каналов связи, так и информации, к которой осуществляется доступ, то есть, за счёт организации параллельных соединений между УИ и УП (рис. 3) [9].

При формировании подобных структур важно определиться с критерием, учитывающим минимальную стоимость используемых сетевых ресурсов и требуемой пользователем доступностью информации.

Пусть $c^{(i)}$ – стоимость i-го соединения между УИ и УП, организованного для обеспечения доступности информации; $P^{(i)}$ – вероятность обеспечения доступности информации i-го соединения ($i = \overline{1,n}$).

Тогда общая стоимость n параллельных соединений составит

$$C_0 = \sum_{i=1}^{n} c^{(i)}.$$

Предположим, что атаки на каждое соединение независимы. В результате общая вероятность обеспечения доступности определяется

$$P_0 = 1 - \prod_{i=1}^{n} \left(1 - P^{(i)}\right).$$

Пусть все n соединений одинаковы по стоимости $c = c^{(i)}$, то есть $C_0 = n \cdot c$ и по вероятности обеспечения доступности информации $P = P^{(i)}$. Тогда

$$Q_0 = (1 - P)^n, \qquad (11)$$

где

$$Q_0 = 1 - P_0.$$

Прологарифмируем выражение (11), результат разделим на $C_0 = n \cdot c$:

$$\ln \frac{Q_0}{C_0} = \frac{\ln(1-P)}{c}. \qquad (12)$$

Из (12) следует вывод, что оптимальным соединением, с точки зрения доступности информации при минимальной стоимости $c^{(i)}$, будет то, у которого максимально следующее отношение:

$$k^{(i)} = \left| \frac{\ln(1-P^{(i)})}{c^{(i)}} \right|.$$

Выводы

1. ***"Гибридная" система шифрования*** является вполне приемлемой для использования в МСС с целью обеспечения конфиденциальности пользовательской информации, однако из-за необходимости наличия у пользователей криптографического обеспечения и знаний в области ЗИ ограничивают её массовое использование.

2. Применение ***метода многопутевой маршрутизации с пороговой схемой разделения сообщения*** обеспечивает конфиденциальность пользовательской информации в МСС. Однако данный метод имеет недостатки – жёсткие требования к количеству одновременно установленных независимых маршрутов и идентичность их ВВХ.

3. Многократное "вложение" криптографических ассиметричных алгоритмов шифрования существенно сокращает время шифрования при сохранении требуемого уровня конфиденциальности информации.

4. ***Криптографический метод с дублированием информации*** для обеспечения целостности значительно влияет на задержку во времени при передаче пользовательской информации. Это ограничивает его применение в МСС для высокоскоростных приложений, функционирующих в реальном масштабе времени.

5. Применение ***метода информационного резервирования и резервирования элементов инфраструктуры*** ТКС позволяет обеспечить комплексную защиту пользовательской информации с QoS высокоскоростных приложений, функционирующих в реальном масштабе времени в МСС.

6. Реализация метода информационного резервирования и резервирования элементов инфраструктуры ТКС для обеспечения комплексной защиты пользовательской информации с QoS возможна за счёт использования ресурсов сетевого уровня МВОС МСС, то есть, процедуры, участвующие в мониторинге инфраструктуры МСС, выборе оптимального маршрута и установлении соединений, позволяют обеспечить не только QoS приложений, но и требуемый уровень информационной безопасности.

7. В этой связи возникает необходимость в разработке, исследовании новых методов маршрутизации, способных решать задачи комплексной защиты пользовательской информации с поддержкой QoS в МСС.

Литература

1. ***Р 50.1.053-2005.*** Рекомендации по стандартизации "Информационные технологии. Основные термины и определения в области технической защиты информации". Введ. 2006-01-01. М.: Изд-во стандартов, 2005. 13 с.

2. ***Рябко Б.Я., Фионов А.Н.*** Основы современной криптографии для специалистов в информационных технологиях. М.: Научный мир, 2004. 173 с.

3. ***Шнайер Б.*** Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Изд-во "Триумф", 2002. 816.

4. ***Кулаков Ю.А., Левчук А.В.*** Многопутевая маршрутизация в беспроводных сетях // Электроника и системы управления. М.: НАУ. № 4 (26), 2010. С. 142-147.

5. ***Lou W., Zhang Y., Liu W., Fang Y.*** SPREAD: Improving network security by multipath routing in mobile ad hoc networks, Wireless Netw, 2009. Vol. 15. P. 279-294.

6. ***Новиков С.Н., Солонская О.И.*** Исследование возможности обеспечения конфиденциальности в мультисервисных сетях связи // Доклады ТУСУР. № 1 (25), ч. 2. 2012. С. 213-215.

7. ***Мелентьев О.Г.*** Теоретические аспекты передачи данных по каналам с группирующимися ошибками М.: Горячая линия – Телеком, 2007. 232 с.

8. ***Новиков С.Н., Солонская О.И.*** Обеспечение целостности в мультисервисных сетях // Доклады ТУСУР. № 1 (19), ч. 2. 2009. С. 83-85.

9. ***Новиков С.Н., Солонская О.И.*** Алгоритм, позволяющий обеспечить требуемый пользователем уровень доступности информации // Свидетельство о регистрации электронного ресурса в объединенном фонде электронных ресурсов "Наука и Образование" института научной информации и мониторинга РАО, № 16227 от 29 сентября 2010 г.

Статья опубликована 25 мая 2013 г.