УДК 004.056.5

С.Н. Новиков

Методологические аспекты защиты информации с использованием ресурсов мультисервисных сетей связи

Предлагаются методологические основы комплексной защиты пользовательской информации (обеспечение конфиденциальности, целостности и доступности) на базе технологий сетевого уровня (протоколов маршрутизации и сигнализации) мультисервисных сетей связи.
Ключевые слова: конфиденциальность, целостность, доступность, маршрутизация.

Одним из путей обеспечения комплексной защиты информации (ЗИ) без снижения QoS является использование ресурсов мультисервисных сетей связи (МСС) (каналов связи, криптографических комплексов, баз данных и т.д.). В этом случае пользователь не обязательно должен обладать знаниями в области ЗИ и иметь специальное программно-аппаратное обеспечение. Ему достаточно определить свой профиль ЗИ (количественные оценки конфиденциальности, целостности и доступности). Система управления, проведя мониторинг свободных ресурсов МСС, реализует не только соединение, поддерживающее QoS для выбранного приложения, но и заявленный пользователем профиль. Реализация данного подхода возможна за счет протоколов маршрутизации и сигнализации.

Обеспечение комплексной ЗИ с использованием ресурсов МСС. В криптосистемах с открытым ключом отсутствует закрытый канал связи, и это упрощает проблему сеансовых ключей. Однако такие алгоритмы имеют особенности: для достижения аналогичной криптостойкости с симметричными алгоритмами требуется более длинный ключ; зависимость времени шифрования от длины ключа L_k имеет нелинейный характер и в общем случае определяется $t_{\text{ш}} = AL_k^c + B$, где $t_{\text{ш}}$ – время зашифрования; A, B и c – постоянные, значения которых определяются криптографическими алгоритмами. Оба фактора значительно ограничивают применение асимметричных криптосистем в МСС, так как существует критичная длина ключа $L_{k\ \text{кр}}$, превышение которой приведет к недопустимому увеличению $t_{\text{ш}}$ и как следствие к снижению QoS высокоскоростных приложений, функционирующих в реальном масштабе времени. *Конфиденциальность информации* и QoS высокоскоростных приложений предлагается обеспечить за счет многократного вложения асимметричных, криптографических алгоритмов шифрования [1]

$$y = E_{k_l}\left\{...E_{k_i}...[E_{k_1}(M)]\right\};\quad M = D_{k_1}\left\{...D_{k_i}[...D_{k_l}(y)]\right\}. \tag{1}$$

Здесь: $y = E_k(M)$, $M = D_k(y)$ – соответственно, зашифрование открытой информации M и расшифрование закрытой информации y с помощью независимых ключей $k_i; i = \overline{1,l}$; l – количество «вложенных» алгоритмов шифрования. Время шифрования (1) с учетом рис. 1 определяется

$$t_{\text{ш сост}} = l\left(\ A\frac{L_{k\ \text{сост}}}{l}\ \right)^c + B = \frac{A^c L_{k\ \text{сост}}^c}{l^{c-1}} + B, \tag{2}$$

при общей длине составного ключа $L_{k_{\text{сост}}} = \sum_{i=1}^{l} L_{k_i}$; $L_{k_i} = \text{const}$. Временной выигрыш применения «составного» ключа по отношению к зашифрованию одним «длинным» составит

$$\frac{t_{\text{ш}}}{t_{\text{ш сост}}} = \frac{AL_{k\ \text{сост}}^c + B}{l\left(A\left(\frac{L_{k\ \text{сост}}}{l}\right)^c + B\right)} = \frac{AL_{k\ \text{сост}}^c + B}{lA\left(\frac{L_{k\ \text{сост}}}{l}\right)^c + lB} = \frac{AL_{k\ \text{сост}}^c}{lA\left(\frac{L_{k\ \text{сост}}}{l}\right)^c} = l^{c-1}. \tag{3}$$

Результаты натурного эксперимента зашифрования алгоритмом RSA блока данных объемом 1 Кбайт при изменении длины ключа от 256 до 2048 бит; использовании составного 256-битного ключа подтвердили теоретическое предположение (3) [2].

Целостность и доступность информации предлагается обеспечить за счет организации n параллельных соединений между узлом-источником (УИ) и узлом-получателем (УП) в МСС [2]. Пусть передаются сообщения $M=\{M_1,M_2\}$ с априорными вероятностями $P(M_1)$ и $P(M_2)$; $P_{\text{м}}^{(i)}$ – вероятность модификации сообщения $M=\{M_1,M_2\}$ в i-м соединении ($i=\overline{1,n}$). Обеспечение целостности информации сводится к процессу принятия решения в точке приема по n одновременно принятым сообщениям $x=(x_1,...,x_i,...,x_n)$. Таким образом, на выходе решающего устройства (РУ) значение M^* будет соответствовать переданному сообщению $M=\{M_1,M_2\}$.

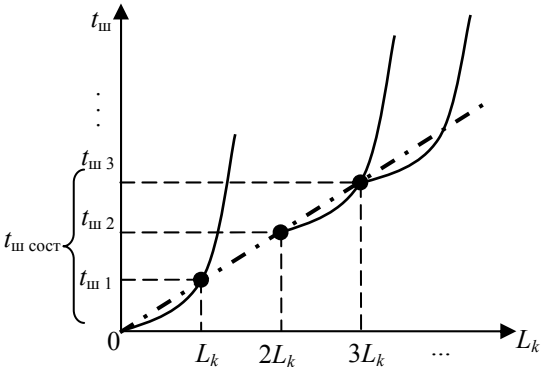

Рис. 1. Зависимости времени зашифрования от длины составного ключа

Условные вероятности, что на выходе РУ будет M_1 или M_2:

$$P\left(M_1/\left(x_i;i=\overline{0,n}\right)\right)=\frac{P(M_1)\left\{\prod\limits_{i\in x_i=M_1}\left(1-P_{\text{м}}^{(i)}\right)\prod\limits_{i\in x_i=M_2}P_{\text{м}}^{(i)}\right\}}{P\left(x_i;i=\overline{0,n}\right)};$$

$$P\left(M_2/\left(x_i;i=\overline{0,n}\right)\right)=\frac{P(M_2)\left\{\prod\limits_{i\in x_i=S_1}P_{\text{м}}^{(i)}\prod\limits_{i\in x_i=S_2}\left(1-P_{\text{м}}^{(i)}\right)\right\}}{P\left(x_i;i=\overline{0,n}\right)}.$$

Возьмем отношение этих выражений, прологарифмируем и обозначим

$$a_0=\ln\frac{P(M_1)}{P(M_2)};\quad a_i=\ln\frac{\left(1-P_{\text{м}}^{(i)}\right)}{P_{\text{м}}^{(i)}}. \tag{4}$$

В результате получим

$$\ln\frac{P\left\{M_1/\left(x_i;i=\overline{0,n}\right)\right\}}{P\left\{M_2/\left(x_i;i=\overline{0,n}\right)\right\}}=a_0+\sum_{i=1}^{n}x_ia_i. \tag{5}$$

Таким образом, правило принятия решения на выходе РУ имеет вид

$$a_0+\sum_{i=1}^{n}x_ia_i\begin{cases}\text{если}>0\Rightarrow M^*=M_1;\\ \text{если}<0\Rightarrow M^*=M_2.\end{cases} \tag{6}$$

Функциональная схема РУ представлена на рис. 2.

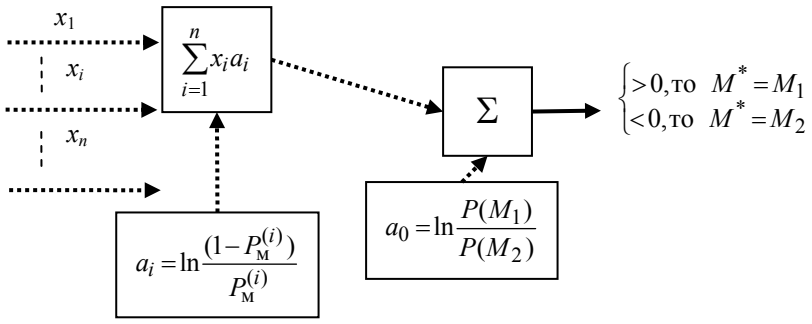

Рис. 2. Функциональная схема РУ

Вероятность целостности информации на выходе РУ при условии, что n – нечетно и $P_{\text{м}} = P_{\text{м}}^{(i)}$; $i = \overline{1,n}$ – независимые события, определяется

$$P_{\text{Ц РУ}} = 1 - \sum_{i=0}^{\frac{n-1}{2}} C_n^{\frac{n+1+2i}{2}} (1-P_{\text{м}})^{\frac{n-1-2i}{2}} P_{\text{м}}^{\frac{n+1+2i}{2}}. \quad (7)$$

Численные оценки целостности информации на выходе решающего устройства представлены на рис. 3. Статистическое моделирование работы РУ подтверждает теоретические расчеты (7).

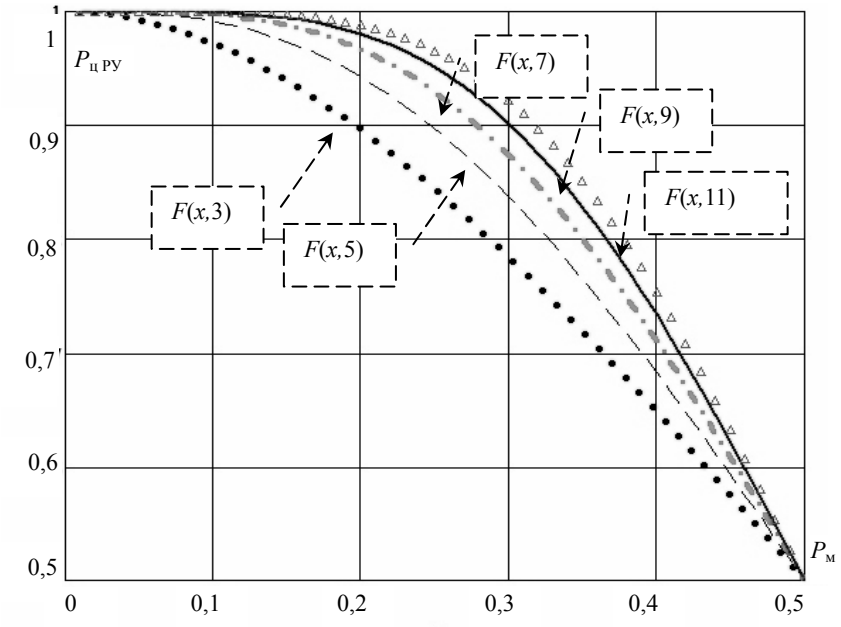

Рис. 3. График $P_{\text{ц РУ}} = f(P_{\text{м}})$ при различных n

Базовым методом обеспечения доступности информации является резервирование и дублирование как самих каналов связи, так и информации, к которой осуществляется доступ, т.е. за счет организации параллельных соединений между УИ и УП информации. В данном случае важно определить *критерий выбора минимальных по стоимости ресурсов МСС* для обеспечения требуемой пользователем доступности информации [3].

Введем обозначения: $c_{\text{Д}}^{(i)}$ – стоимость i-го соединения между УИ и УП, организованного для обеспечения доступности информации; $P_{\text{Д}}^{(i)}$ – вероятность обеспечения доступности информации i-го соединения ($i = \overline{1,n}$). Тогда общая стоимость организации параллельных соединений составит

$$c_{\text{Д}} = \sum_{i=1}^{n} c_{\text{Д}}^{(i)}. \quad (8)$$

Предположим, что атаки на каждое соединение независимы. Тогда результирующая вероятность обеспечения доступности определяется выражением

$$P_{\text{Д}}^{(\text{рез})} = 1 - \prod_{i=1}^{n} \left(1 - P_{\text{Д}}^{(i)}\right). \quad (9)$$

Обозначим

$$Q_{\text{Д}}^{(i)} = 1 - P_{Д}^{(i)},\ Q_{\text{Д}}^{(\text{рез})} = 1 - P_{\text{Д}}^{(\text{рез})}. \quad (10)$$

Тогда

$$Q_{\text{Д}}^{(\text{рез})} = \left[Q_{\text{Д}}^{(i)} \right]^n. \quad (11)$$

Прологарифмируем обе части выражения (11):

$$\ln Q_{\text{Д}}^{(\text{рез})} = n \ln Q_{\text{Д}}^{(i)}. \quad (12)$$

Допустим, что все параллельные соединения одинаковы по стоимости:

$$c_{\text{Д}} = n c_{\text{Д}}^{(i)}. \quad (13)$$

Разделим (12) на $c_{\text{Д}}$, с учетом (13) и (10) получим

$$\ln \frac{Q_{\text{Д}}^{(\text{рез})}}{c_{\text{Д}}} = \frac{\ln\left(1 - P_{\text{Д}}^{(i)}\right)}{c_{\text{Д}}^{(i)}}. \quad (14)$$

Из (14) следует вывод, что оптимальным соединением с точки зрения доступности информации при минимальной стоимости $c_{\text{Д}}^{(i)}$ будет то, у которого следующее отношение максимально:

$$k_{\text{Д}}{}^{(i)} = \left| \frac{\ln(1 - P_{\text{Д}}^{(i)})}{c_{\text{Д}}{}^{(i)}} \right|. \quad (15)$$

Методика комплексной ЗИ. Реализация вышеизложенного подхода, обеспечивающего комплексную ЗИ, возможна за счет механизмов сетевого уровня МСС [4, 7] (протоколов маршрутизации и сигнализации) (рис. 4).

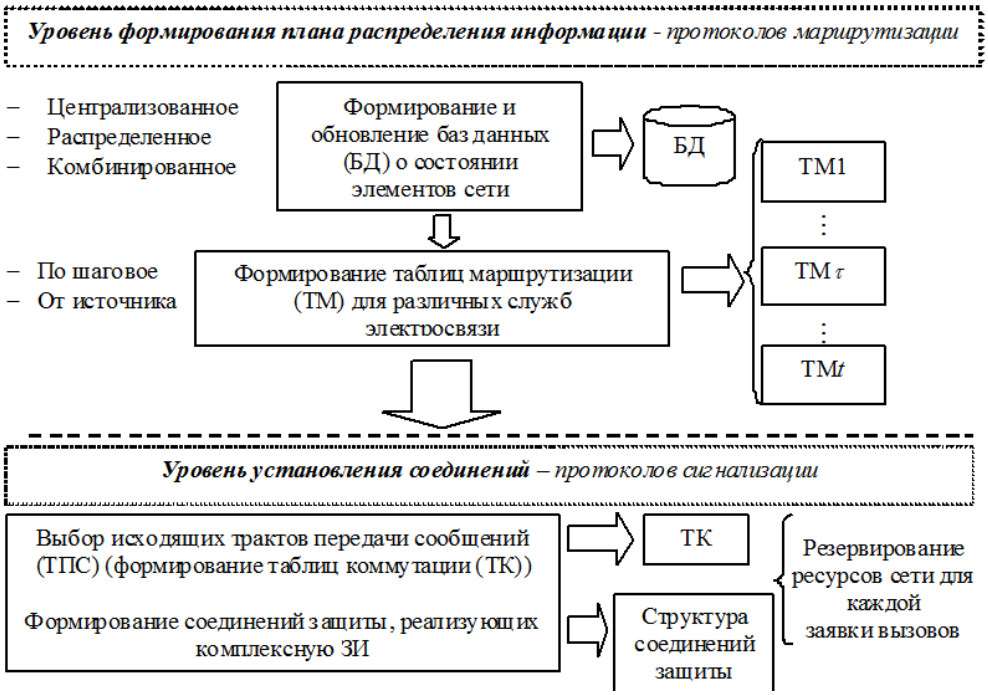

Рис. 4. Обобщенная функциональная модель маршрутизации в МСС

Основным продуктом уровня формирования ПРИ являются ТМ для каждой службы электросвязи $\left(\tau = \overline{1,t}\right)$ (приложения МСС). При этом применяются соответствующие методы мониторинга МСС, формирования и коррекции БД, которые по степени централизации можно классифицировать на централизованные, распределенные и комбинированные.

Уровень сигнализации, используя методы выбора исходящих ТПС, по сформированным ТМ формирует во всех транзитных узлах коммутации (УК), начиная с узла-источника (УИ):

– ТК для каждой заявки на установление соединения с требуемым QoS приложений МСС;

– структуру соединений защиты с целью выполнения требований пользователей к степени защищенности передаваемой информации (конфиденциальности, доступности, целостности).

Передача сообщений пользователей осуществляется по таблицам коммутации, которые сформированы на уровне системы сигнализации.

Таким образом, протоколы сетевого уровня (маршрутизации и сигнализации), проведя мониторинг свободных ресурсов МСС, реализуют не только соединение, поддерживающее QoS для выбранного приложения, но и заявленный пользователем профиль комплексной ЗИ.

Математическая модель анализа маршрутизации в МСС. В работе [4] проведена попытка систематизировать и обобщить известные решения, реализованные в технологиях IP, ATM и MPLS. В результате была предложена новая классификация методов маршрутизации, позволяющая, комбинируя известные методы формирования ПРИ и выбора исходящих ТПС, разработать новые методы маршрутизации.

«Логико-статистический» – сочетание «логического» и «статистического» методов формирования ПРИ. В условиях отсутствия внешних деструктурирующих воздействий на МСС формирование ПРИ осуществляется «статистическим» методом. В условиях резкого изменения структуры МСС (по каким-либо причинам) применяется «логический» метод.

«Логико-лавинный» – сочетание «лавинного» и «логического» методов состоит в том, что для установления оптимального соединения из УИ организуется «лавинный» поиск, но не во всех направлениях, а лишь в сторону УП. Волна поиска при этом распространяется в пределах некоторой зоны в виде полосы, охватывающей УИ и УП. Ширина, форма полосы зависят от приоритета пользователя, состояния элементов сети, требований приложений к QoS и могут устанавливаться в различных пределах. В частности, для пользователей низшей категории количество выбранных ТПС может не превышать одного, тогда поиск превращается в «чисто» последовательный.

«Логико-лавинно-статистический» – обобщение «логического», «лавинного» и «статистического». Применение одного из перечисленных методов зависит от условий функционирования МСС. В условиях отсутствия внешних деструктурирующих воздействий на МСС формирование ПРИ осуществляется «статистическим» методом. В условиях резкого изменения структуры МСС (по каким либо причинам) применяется «логико-лавинный» метод.

В этой связи с целью определения оптимальных методов маршрутизации возникает необходимость в разработке математической модели [5] функционирования МСС в условиях внешних деструктурирующих воздействий.

Структуру МСС представим в виде неориентированного графа $G[A_S, M_S]$ с множеством: вершин $A_S = \{a_i\};\ i = \overline{1,S}$ – УК; ребер $M_S = \{m_{ij}\};\ i,j = \overline{1,S};\ i \neq j$ – линий связи (ЛС). ПРИ в МСС задается в виде набора векторов

$$P^{(j)} = \left\| p_{i,v}^{(j)} \right\|_{(S-1),H_j} = \left(\overline{p_1^{(j)}}, \ldots, \overline{p_i^{(j)}}, \ldots, \overline{p_{j-1}^{(j)}}, \overline{p_{j+1}^{(j)}}, \ldots, \overline{p_S^{(j)}} \right), \quad (16)$$

где $P_{\overline{i}}^{(j)} = (p_{i,v}^{(j)});\ \sum_{v=1}^{H_j} p_{i,v}^{(j)} v = \overline{1,H_j};\ i,j = \overline{1,S};$ H_j – степень a_j-го УК. Элементы вектора $\overline{p_i^{(j)}}$ определяют вероятность того, что на этапе поиска маршрута к a_j-му УП в a_i-м транзитном УК, начиная с УИ, будет выбрана v-я исходящая ЛС. Выражение (16) и процедура выбора исходящих ТПС определяют метод маршрутизации (M).

Поступающий в МСС поток данных τ-го приложения считается самоподобным

$$f(x) = \begin{cases} \dfrac{\lambda_{\tau,R,T}^{H_\tau} \cdot x^{H_\tau - 1} \cdot e^{-\lambda_{\tau,R,T} \cdot x}}{\Gamma(H_\tau)}; R,T = \overline{1,S}; R \neq T; \tau = \overline{1,t}; x \geq 0; \\ 0, \qquad\qquad x < 0, \end{cases}$$

где $\Gamma(H_\tau) = \int_0^\infty x^{H_\tau - 1} e^{-t} dx$ – гамма-функция с параметрами: $\lambda_{\tau,R,T}$ – интенсивность поступления потока данных τ-го приложения в a_R-й УИ для передачи в a_T-й УП; $0{,}5 < H_\tau \leq 1$ – параметр Херста. Интенсивность потока данных τ-го приложения составит $\lambda_\tau = \sum_{R,T=1}^{S} \lambda_{\tau,R,T}$. Вероятность поступления потока данных τ-го приложения в a_R-й УИ для его последующей передачи a_T-му УП будет

$$\Pi\tau=\left\|\pi_{\tau,R,T}\right\|_{S,S};\ \ 0\le\pi_{\tau,R,T}=\frac{\lambda_{\tau,R,T}}{\lambda_\tau}\le 1;\ \ \sum_{R,N=1}^{S}\pi_{\tau,R,T}=1;\ \ \tau=\overline{1,t}.$$

Длительность обслуживания входящего потока данных τ-го приложения подчиняется экспоненциальному закону с параметром μ_τ. Критерием оценки качества функционирования МСС принята

$$\{\hat{P}^{\tau}_{\text{отк}};\ \hat{p}^{(R,T)\tau}_{\text{отк}}\}=f\{G[A_S,M_S];\ \Pi_\tau;\ \lambda_\tau;\ \mu_\tau;\ M\};\ \ R,T=\overline{1,T};\ \ R\ne T;\ \ \tau=\overline{1,t}\ ; \qquad (17)$$

$\hat{P}^{(R,T)\tau}_{\text{отк}};\ R,T=\overline{1,T};\ R\ne T;\ \tau=\overline{1,t}$ – вероятность отказа в обслуживании τ-го приложения между УИ (a_R) и УП (a_T) – дифференциальная оценка; $\hat{P}^{\tau}_{\text{отк}}$ – вероятность отказа в обслуживании τ-го приложения в среднем по сети – интегральная оценка.

Методика оценки (17) состоит в решении следующей системы уравнений (18):

$$\left\{\begin{array}{l}
P^{(M)}_{(T)}=\left\|p^{(M)j}_{(T)i}\right\|_{S,S};\ \ i,j=\overline{1,S};\ \ i\ne j;\\
\lambda^{(M)j}_{0\ \tau,i}=\lambda_\tau\cdot\sum\limits_{T=1}^{S}p^{(M)j}_{(T)i}\cdot\pi_{\tau,i,j};\quad i,j=\overline{1,S};i\ne j;\\
p^{(M)j}_{\tau,i}=\dfrac{\left(1-\dfrac{\rho^{(M)}_{\tau,i,j}}{4}-\sqrt{\dfrac{\rho^{(M)}_{\tau,i,j}{}^2}{16}+\dfrac{\rho^{(M)}_{\tau,i,j}}{2}}\right)}{1-\left(\dfrac{\rho^{(M)}_{\tau,i,j}}{4}+\sqrt{\dfrac{\rho^{(M)}_{\tau,i,j}{}^2}{16}+\dfrac{\rho^{(M)}_{\tau,i,j}}{2}}\right)^2}\left(\dfrac{\rho^{(M)}_{\tau,i,j}}{4}+\sqrt{\dfrac{\rho^{(M)}_{\tau,i,j}{}^2}{16}+\dfrac{\rho^{(M)}_{\tau,i,j}}{2}}\right);\\
P^{\tau}_{\text{отк}}=\sum\limits_{k=1}^{2^n}Q^{(k)}_{\text{o}}\cdot\prod\limits_{\nu=1}^{n}\left(q_\nu^{\sigma_\nu}\cdot p_\nu^{1-\sigma_\nu}\right);\ \ R,T=\overline{1,S};\ \ \tau=\overline{1,t}\ ;\\
P^{(R,T)\tau}_{\text{отк}}=\sum\limits_{k=1}^{2^n}Q^{(k)}_{RT}\cdot\prod\limits_{\nu=1}^{n}\left(q_\nu^{\sigma_\nu}\cdot p_\nu^{1-\sigma_\nu}\right);\ \ R,T=\overline{1,S};\ \ \tau=\overline{1,t}\ .
\end{array}\right. \qquad (18)$$

Здесь $p^{(M)j}_{(T)i}$ – вероятность перехода из состояния a_i в a_j конечной цепи Маркова (КЦМ) для M-го метода маршрутизации при поиске a_T-го УК; a_T – поглощающее, т.е. $p^{(M)T}_{(T)T}=1$; $P^{(M)}_{(T)}=\left\|p^{(M)j}_{(T)i}\right\|_{S,S}$ – матрица переходных вероятностей (КЦМ); $\lambda^{(M)j}_{0\ \tau,i}=\lambda_\tau\cdot\sum\limits_{T=1}^{S}p^{(M)j}_{(T)i}\cdot\pi_{\tau,i,j}=\sum\limits_{T=1}^{S}\lambda^{(M)j}_{(T)\tau,i};\ \overline{1,S};\ i\ne j$ – общая интенсивность потоков τ-го приложения в $m_{i,j};\ i,j=\overline{1,S};\ i\ne j$; $\lambda^{(M)j}_{(T)\tau,i}=p^{(M)j}_{(T)i}\cdot\lambda_{\tau,i,T};\ i,j=\overline{1,S};\ i\ne j$ – интенсивность потока τ-го приложения в $m_{i,j};\ i,j=\overline{1,S};\ i\ne j$ при поиске a_T-го УК M-м методом маршрутизации; $p^{(M)j}_{\tau,i}$ – вероятность отказа в обслуживании τ-го приложения в $m_{i,j};\ i,j=\overline{1,S};\ i\ne j$ определяется по формуле, предложенной в [6]; n – количество ребер графа $G[A_S,M_S]$; $k=\overline{1,2^n}$ – количество состояний графа $G[A_S,M_S]$; $Q^{(k)}_o$ и $Q^{(k)}_{ij}$ переменные, принимающие значения 1, если граф, находясь в k-м, соответственно, будет «связен» – обеспечивает связность вершин a_i и a_j. В противном случае переменные равны 0.

Анализ результатов решения системы уравнений (18) методом статистического моделирования позволяет сделать вывод – в условиях выхода элементов МСС из строя более 30% параллельных методов маршрутизации показывают лучшую оценку параметра (17).

Заключение. На основе проведенных исследований возможно сделать следующие выводы:

– Разработаны методологические основы комплексной защиты пользовательской информации (обеспечение конфиденциальности, целостности и доступности) на базе технологий сетевого уровня (протоколов маршрутизации и сигнализации) мультисервисных сетей связи.

– Разработана математическая модель функционирования МСС в условиях внешних деструктурирующих воздействий и самоподобного трафика.

– В условиях выхода элементов МСС из строя более 30% параллельных методов маршрутизации дают лучшую оценку вероятности отказа в обслуживании приложений между УИ и УП.

Литература

1. Алгоритм, позволяющий обеспечить требуемый пользователем уровень конфиденциальности информации в мультисервисных сетях связи / С.Н. Новиков, О.И. Солонская: Свидетельство о регистрации электронного ресурса в объединенном фонде электронных ресурсов «Наука и образование» Института научной информации и мониторинга РАО, № 16462 от 6 декабря 2010 г., ВНТИЦ инв. № 50201050230 от 08.12.2010 г.

2. Пат. 2 513 725 РФ, МПК G 06 F 11/00. Способ обеспечения целостности передаваемой информации / С.Н. Новиков, О.И. Солонская (РФ). – № 2 012 122 695 / 08; заявл. 01.06.12; опубл. 20.04.14. – Бюл. № 11. – 17 с.

3. Алгоритм, позволяющий обеспечить требуемый пользователем уровень доступности информации / С.Н. Новиков, О.И. Солонская: 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., ВНТИЦ инв. № 50201001615 от 05.10.2010 г.

4. Новиков С.Н. Классификация методов маршрутизации в мультисервисных сетях связи // Вестник СибГУТИ. – 2013. – № 2 (25). – С. 92–96.

5. Novikov S.N. The Analysis of Probability Time Characteristics of a Telecommunication Network / S.N. Novikov, A.A. Burov // The IEEE International Siberian Conference on Control and Communications (SIBCON-2005). – Russia, Tomsk, 2005. – P. 26–29.

6. Самоподобие в системах массового обслуживания с ограниченным буфером / М.Н. Петров, Д.Ю. Пономарев // Электросвязь. – 2002. –№ 2. – С. 35–39.

7. Исхаков С.Ю. Разработка методического и программного обеспечения для мониторинга работы локальных сетей / С.Ю. Исхаков, А.А. Шелупанов // Телекоммуникации. – 2013. – № 6. – С. 16–20.

Новиков Сергей Николаевич
Канд. техн. наук, доцент, зав. каф. безопасности и управления в телекоммуникациях СибГУТИ,
г. Новосибирск
Тел.: +7 (383) 269-82-45
Эл. почта: snovikov@ngs.ru

Novikov S.N.

Methodological aspects of data protection with the use of resources multiservice networks

The methodological basis of complex protection of user information (ensuring the confidentiality, integrity and availability) technology-based cross-tevogo level (routing and signaling protocols) multiservice networks are proposed.

Keywords: confidentiality, integrity, availability, routing.