СибГУТИ Кафедра «Безопасность и управление в телекоммуникациях» (БиУТ) 2006 г. – 2016 г.

СибГУТИ Кафедра «Безопасность и управление в телекоммуникациях» (БиУТ) 2006 г. – 2016 г.

СибГУТИ Кафедра «Безопасность и управление в телекоммуникациях» (БиУТ)
2006 г. – 2016 г.

Научные направления БиУТ

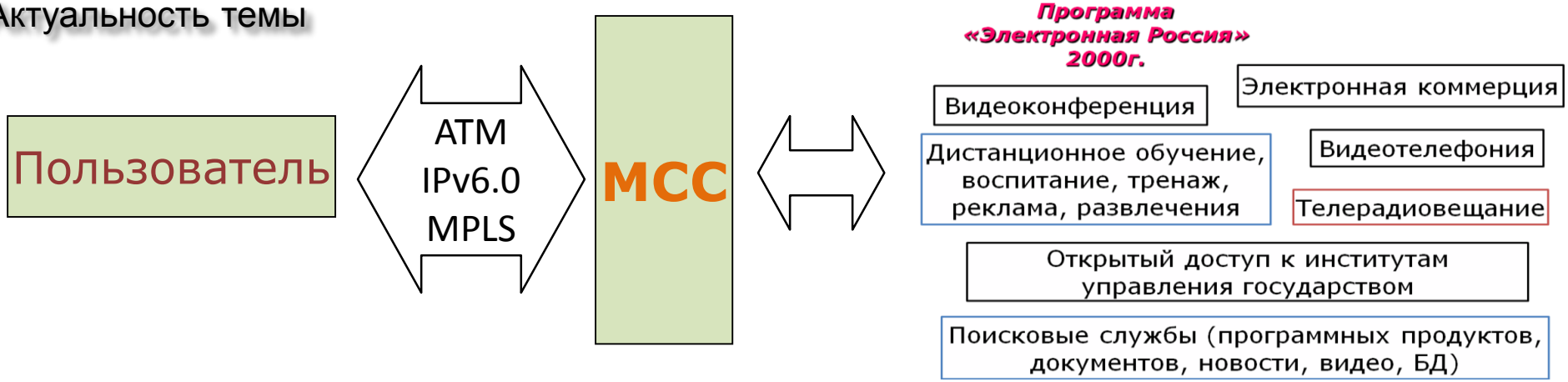
1. Оценка качества профессиональной деятельности и выбора экспертов в любых отраслях производства и оказания услуг.

2. Оценки рисков несанкционированного доступа и защищенности объектов информатизации.

3. Мультибиометрической идентификации личности.

4. Юрисметрия.

5. ЗАЩИТА ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ РЕСУРСОВ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ СВЯЗИ.



Проблемы обеспечения ИБ в МСС

1. ***Со стороны МСС***

Влияние средств защиты информации на QoS

$$\downarrow V;\uparrow t_{зад.\ пи};\uparrow t_{дж.}$$

2. ***Со стороны пользователей***

Наличие и поддержание в актуальном (обновленном) состоянии ***средств защиты информации***, обеспечивающих конфиденциальность, доступность и целостность информации **В УСЛОВИЯХ ВНЕШНИХ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ НА ЭЛЕМЕНТЫ МСС**

Предложение по решению проблемы обеспечения ИБ в МСС

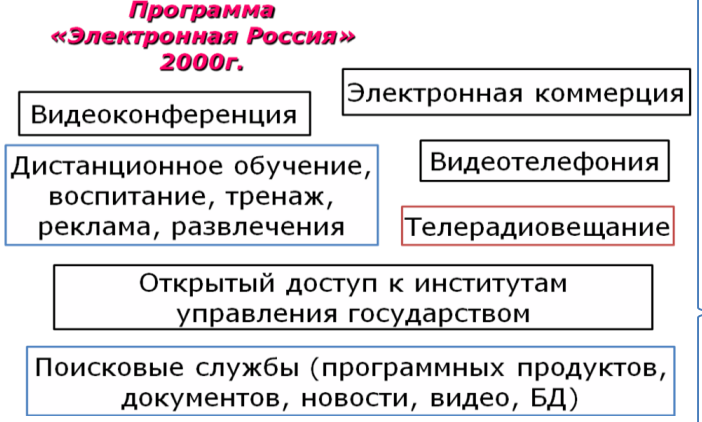
ИСПОЛЬЗОВАТЬ ТЕРРИТОРИАЛЬНО-РАСПРЕДЕЛЕННЫЕ РЕСУРСЫ МСС

(КАНАЛЫ СВЯЗИ, КРИПТОГРАФИЧЕСКИЕ ПРОГРАММНО-АППАРАТНЫЕ КОМПЛЕКСЫ, БАЗЫ ДАННЫХ и т.д.)

Пользователь

Определяет:

1. *Приложение* МСС



2. *Профиль ЗИ*

(количественные/качественные параметры ИБ: доступность, конфиденциальность, целостность)

Система управления МСС

1. Проводит *мониторинг свободных ресурсов* МСС;
2. Реализует:
   - *соединение, поддерживающее* QoS для выбранного приложения;
   - *профиль ЗИ*

Реализация за счет

МЕХАНИЗМОВ СЕТЕВОГО УРОВНЯ МОДЕЛИ ВОС: ПРОТОКОЛОВ **МАРШРУТИЗАЦИИ И СИГНАЛИЗАЦИИ**

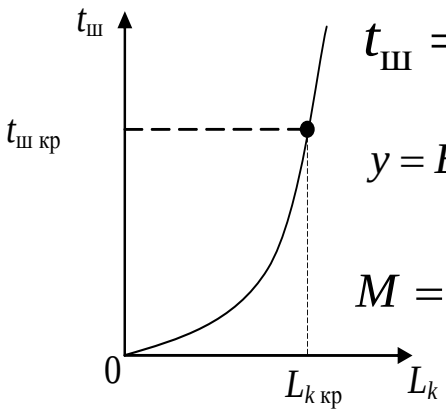
Анализ основных подходов конфиденциальности информации

<table>
<tr><th></th><th>Способ обеспечения конфиденциальности</th><th>Достоинства</th><th colspan="2">Недостатки</th></tr>
<tr><td>1</td><td>Симметричная система шифрования</td><td>Высокая скорость шифрования $t_{ш} = A \cdot L_k + B$</td><td>Наличие закрытого канала связи.</td><td rowspan="3">Пользователи должны иметь дополнительное специальное криптографическое программно-аппаратное обеспечение.</td></tr>
<tr><td>2</td><td>Ассиметричная система шифрования</td><td>Отсутствие закрытого канала связи.</td><td>Низкая скорость шифрования $t_{ш} = AL_k^c + B$</td></tr>
<tr><td>3</td><td>«Гибридная» система шифрования</td><td>1. Отсутствие закрытого канала связи.
2. Высокая скорость шифрования $t_{ш} = AL_k + B$
3. Обеспечивается QoS приложений пользователя.</td><td></td></tr>
<tr><td>4</td><td>Многопутевая маршрутизация с пороговой схемой разделения сообщения</td><td>1. Пользователи не должны иметь дополнительное, специальное, криптографическое, программно-аппаратное обеспечение.
2. Обеспечивается QoS приложений пользователя.</td><td colspan="2">1. Чувствительность к модификации частей секретного сообщения.
2. Необходимость реализации независимых маршрутов с одинаковыми вероятностно-временными характеристиками.</td></tr>
</table>

Исследование возможности использования многократного ассиметричного шифрования

Соответствие криптостойкости алгоритмов шифрования

Алгоритмы	Длины ключей				
Симметричные	56	64	80	112	256
Асимметричные	384	512	768	1792	2304

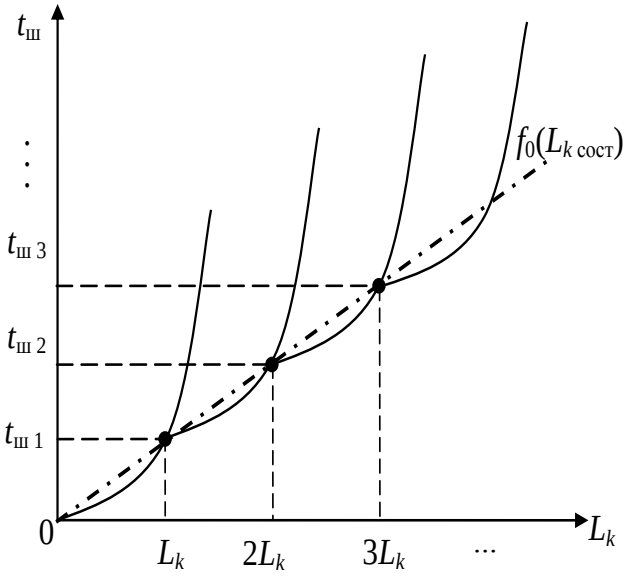


$$t_ш = A \cdot L_k^c + B$$

$$y = E_{k_l}\left\{...E_{k_i}...[E_{k_1}(M)]\right\}$$

$$M = D_{k_1}\left\{...D_{k_i}[...D_{k_l}(y)]\right\}$$

Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: Издательство Триумф, 2002. – 816 с.



Зависимости времени, затрачиваемого на шифрование, от длины составного ключа

***RSA* блок данных объемом 1 Кбайт**
Составной ключ 256 бит

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

Алгоритм, позволяющий обеспечить требуемый пользователем уровень конфиденциальности информации в мультисервисных сетях связи : свидетельство об отраслевой регистрации разработки № 16462 / С. Н. Новиков, О. И. Солонская. – № 50201050230 ; заявл. 06.12.2010 ; опубл. 08.12.2010. – 1 с.

Основные методы, обеспечивающие целостность информации в ТКС

Методы, обеспечивающие целостность информации

Резервирование информации

Криптографические с дублирование информации

Параллельная передача информации по нескольким маршрутам и принятие решения о целостности информации на приемной стороне

Хеширование

Электронная цифровая подпись

Введение в сообщение проверочной комбинации, которая вычисляется по определенным алгоритмам и является «индикатором» нарушения целостности информации

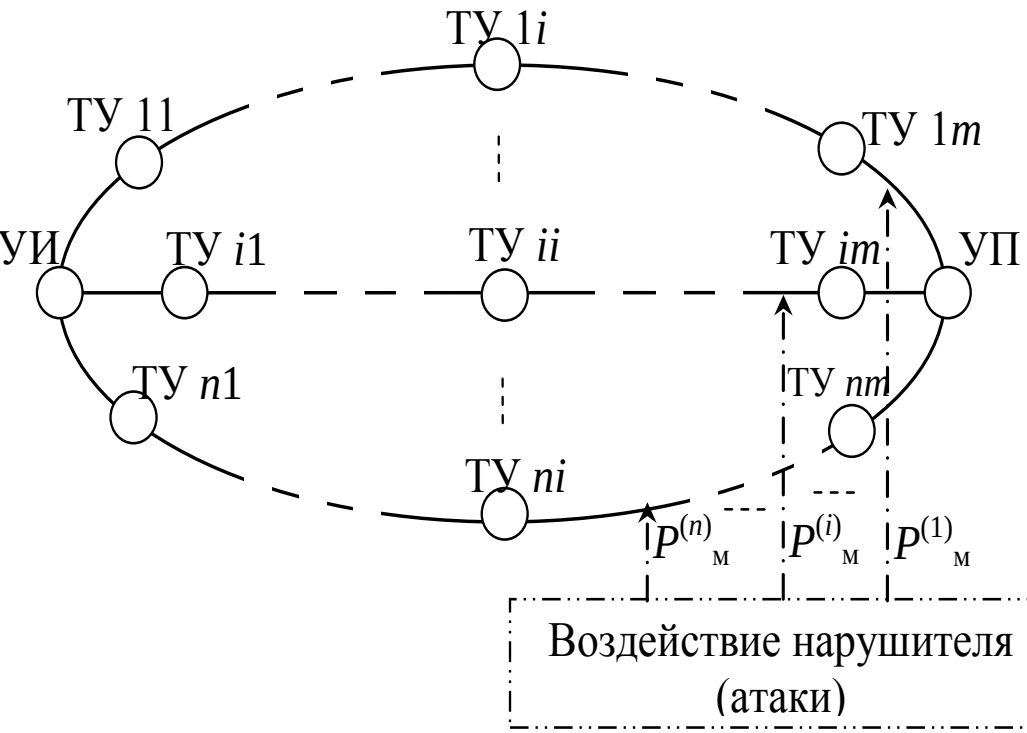
Данный подход только **контролирует целостность информации.** В случае ее модификации источнику необходимо сделать повторную передачу сообщения

И.С. Андронов, У. Пирс, А.А. Сикарев, А.И. Фалько, Л.М. Финк, В.Г. Хорошевский и многие др. ученые

$t_З \Rightarrow$ QoS высокоскоростных приложений МСС, функционирующих в реальном масштабе времени

$t_З \Rightarrow$ ~~QoS~~ высокоскоростных приложений МСС, функционирующих в реальном масштабе времени

Метод обеспечения целостности пользовательской информации на сетевом уровне мультисервисных сетей связи



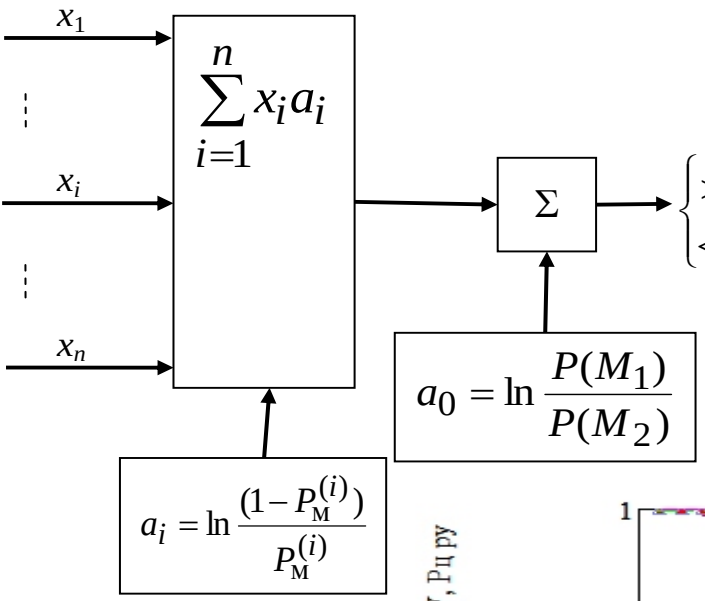
$$P\left(M_1/\left(x_i;i=\overline{0,n}\right)\right)=\frac{P(M_1)\left\{\prod_{i\in x_i=M_1}\left(1-P_{м}^{(i)}\right)\prod_{i\in x_i=M_2}P_{м}^{(i)}\right\}}{P\left(x_i;i=\overline{0,n}\right)}$$

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

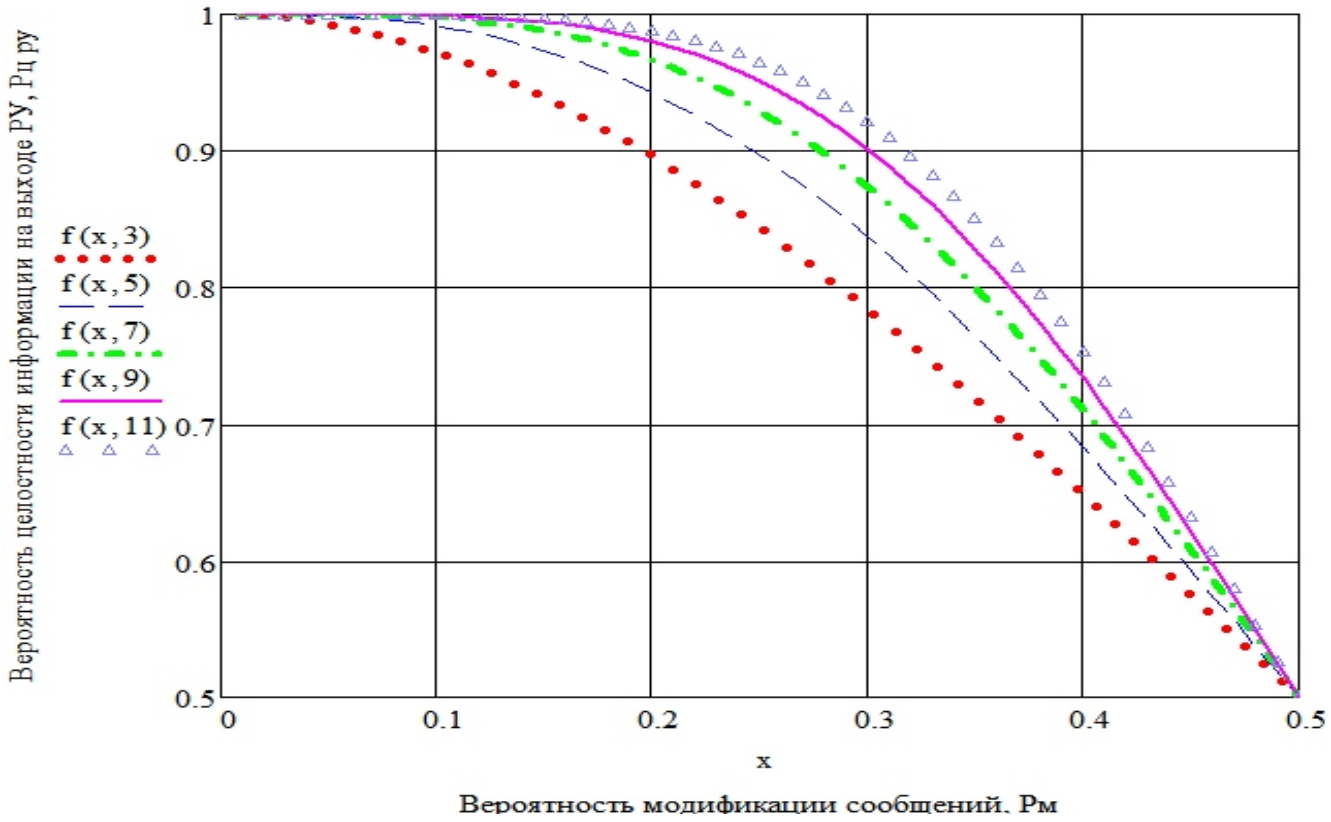
$$\ln\frac{P\left\{M_1/\left(x_i;i=\overline{0,n}\right)\right\}}{P\left\{M_2/\left(x_i;i=\overline{0,n}\right)\right\}}=\ln\frac{P(M_1)}{P(M_2)}+\sum_{i\in x_i=M_1}\ln\frac{\left(1-P_{\text{і}}^{(i)}\right)}{P_{\text{і}}^{(i)}}+\sum_{i\in x_i=M_2}\ln\frac{P_{\text{і}}^{(i)}}{\left(1-P_{\text{і}}^{(i)}\right)}$$

$$a_0+\sum_{i=1}^{n}x_i\cdot a_i\begin{cases}\text{если}>0\Rightarrow M^*=M;_1\\ \text{если}<0\Rightarrow M^*=M_2.\end{cases}$$

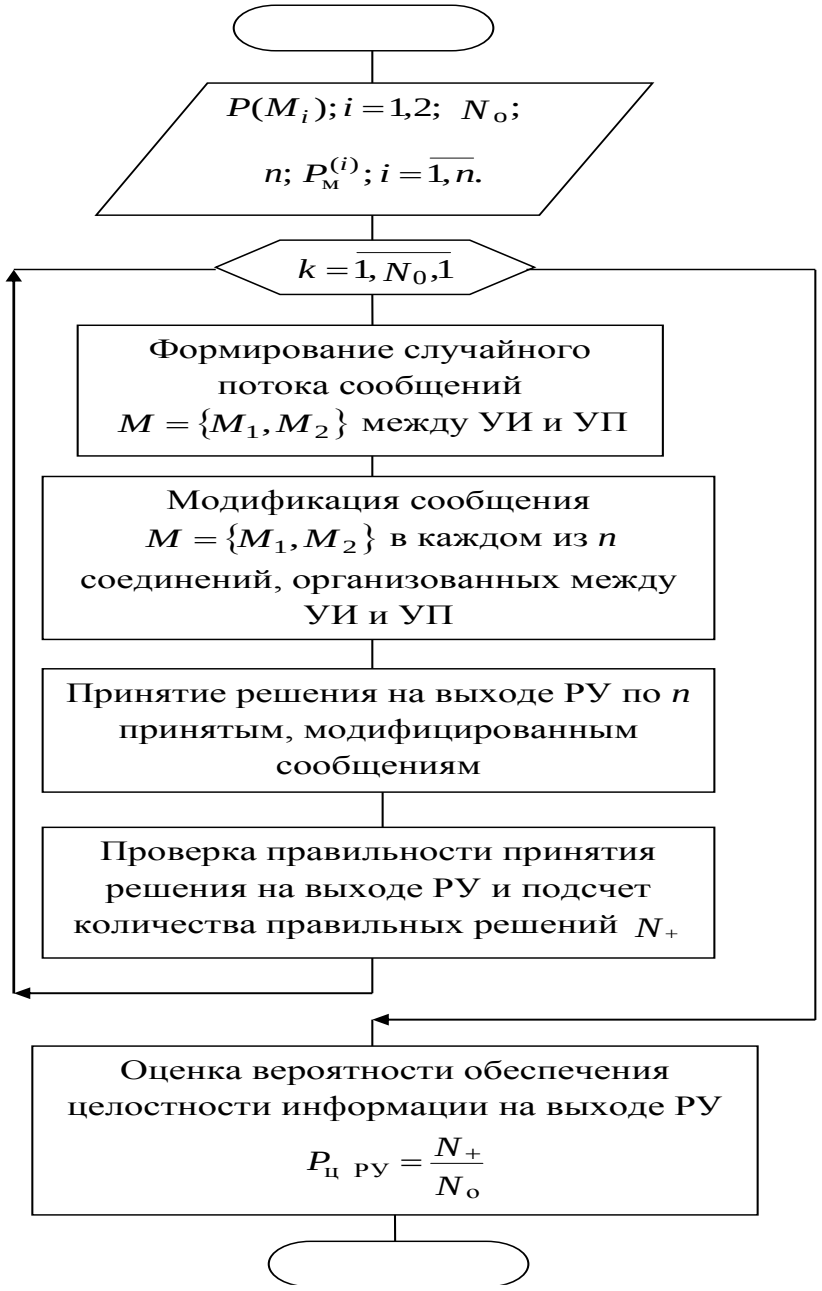
Способ обеспечения целостности передаваемой информации : **пат. 2513725** Рос. Федерация / С. Н. Новиков, О. И. Солонская. – Опубл. 20.04.14, Бюл. № 11.



$$P_{ц\,РУ} = 1 - \sum_{i=0}^{(n-1)/2} C_n^{(n+1+2\cdot i)/2} \cdot (1 - P_м)^{(n-1-2\cdot i)/2} \cdot P_м^{(n+1+2\cdot i)/2}$$



Имитационное моделирование обеспечения целостности ПИ на сетевом уровне МСС



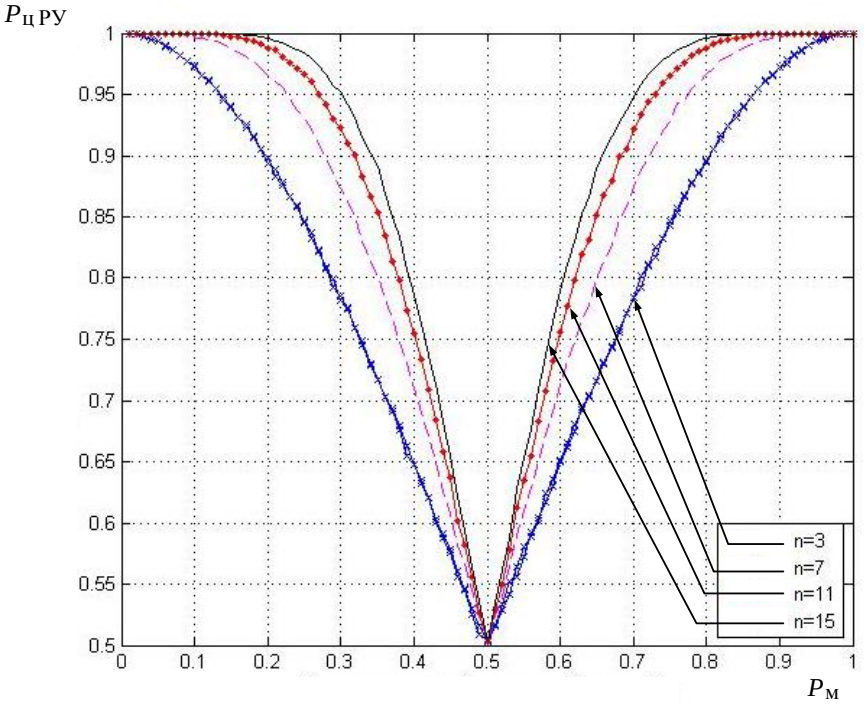
1 Этап

2 Этап

3 Этап

4 Этап

5 Этап



Результаты имитационного моделирования работы РУ
$P_{ц\,РУ} = f(P_м)$ для различных значений n

MatLab

$$\Delta_a = N_o^{-0,5} \cdot \sigma \cdot t_\beta,$$

$$\sigma^2 = P_{ц\,РУ} \cdot (1 - P_{ц\,РУ});$$

$$N_o = 30000, \quad t_\beta = 3,29 \quad \beta = 0,999 \quad \Delta_a \le 0,01.$$

Разработка критерия выбора ресурсов МСС для обеспечения целостности и доступности информации

$$P_{\text{рез}} = 1 - \prod_{i=1}^{n}(1 - p_i) \qquad Q_{\text{рез}} = q_i^n; i = \overline{1,n}. \qquad C_{\text{о}} = n \cdot c_i; i = \overline{1,n};$$

$$\ln Q_{\text{рез}} = n \cdot \ln q_i; i = \overline{1,n} \qquad \frac{\ln Q_{\text{рез}}}{C_{\text{о}}} = \frac{\ln q_i}{c_i}; i = \overline{1,n}.$$

Учитывая, что $\frac{\ln Q_{\text{рез}}}{C_{\text{о}}} = \frac{\ln q_i}{c_i} \le 0; i = \overline{1,n},$ то примем: $\left|\frac{\ln Q_{\text{рез}}}{C_{\text{о}}}\right| = \left|\frac{\ln q_i}{c_i}\right|; i = \overline{1,n}.$

$$\max\left\{\alpha_i = \left|\frac{\ln(1-p_i)}{c_i}\right|; i = \overline{1,n}\right\}$$

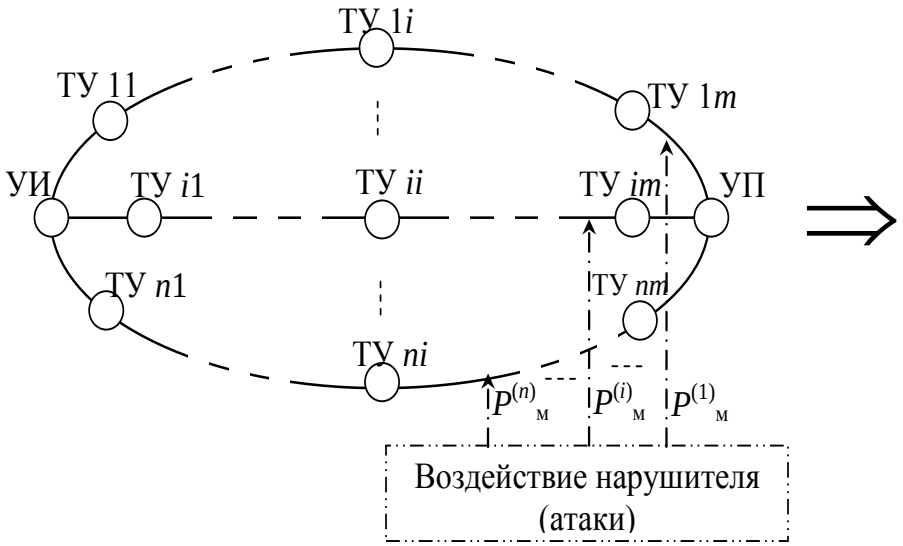
Критерий позволяет выбирать оптимальные, независимые соединения с точки зрения обеспечения целостности и доступности передаваемой информации в МСС при минимальной стоимости

Алгоритм, позволяющий обеспечить требуемый пользователем уровень доступности информации : свидетельство об отраслевой регистрации разработки № 16227 / С. Н. Новиков, О. И. Солонская. – № 50201001615 ; заявл. 29.09.2010 ; опубл. 05.10.2010. – 1 с.

Выводы

$$y = E_{k_l}\left\{...E_{k_i}...[E_{k_1}(M)]\right\}; M = D_{k_1}\left\{...D_{k_i}[...D_{k_l}(y)]\right\} \Rightarrow \downarrow t$$

Передачи пользовательской информации

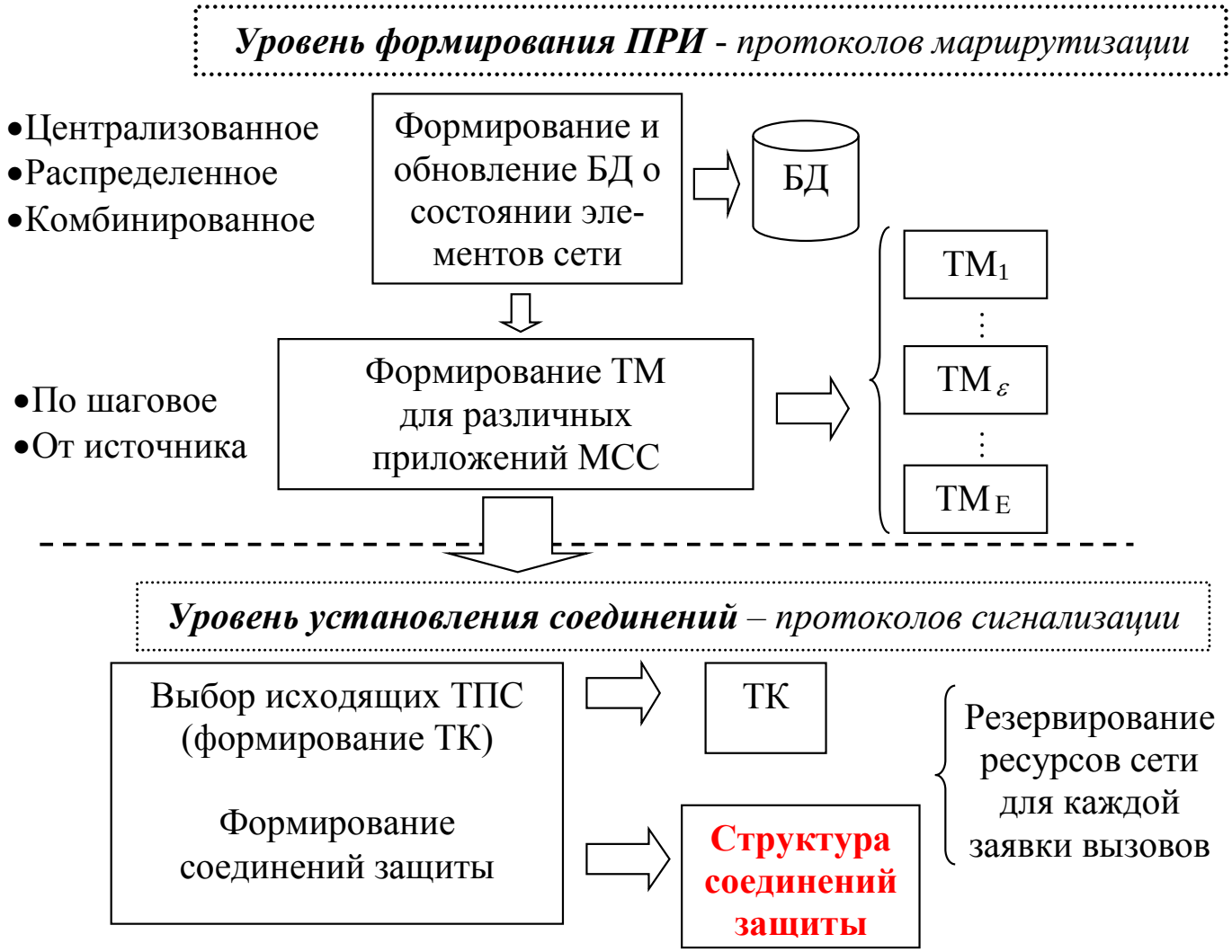


$\Rightarrow$

Обеспечивает доступность и целостность информации в МСС

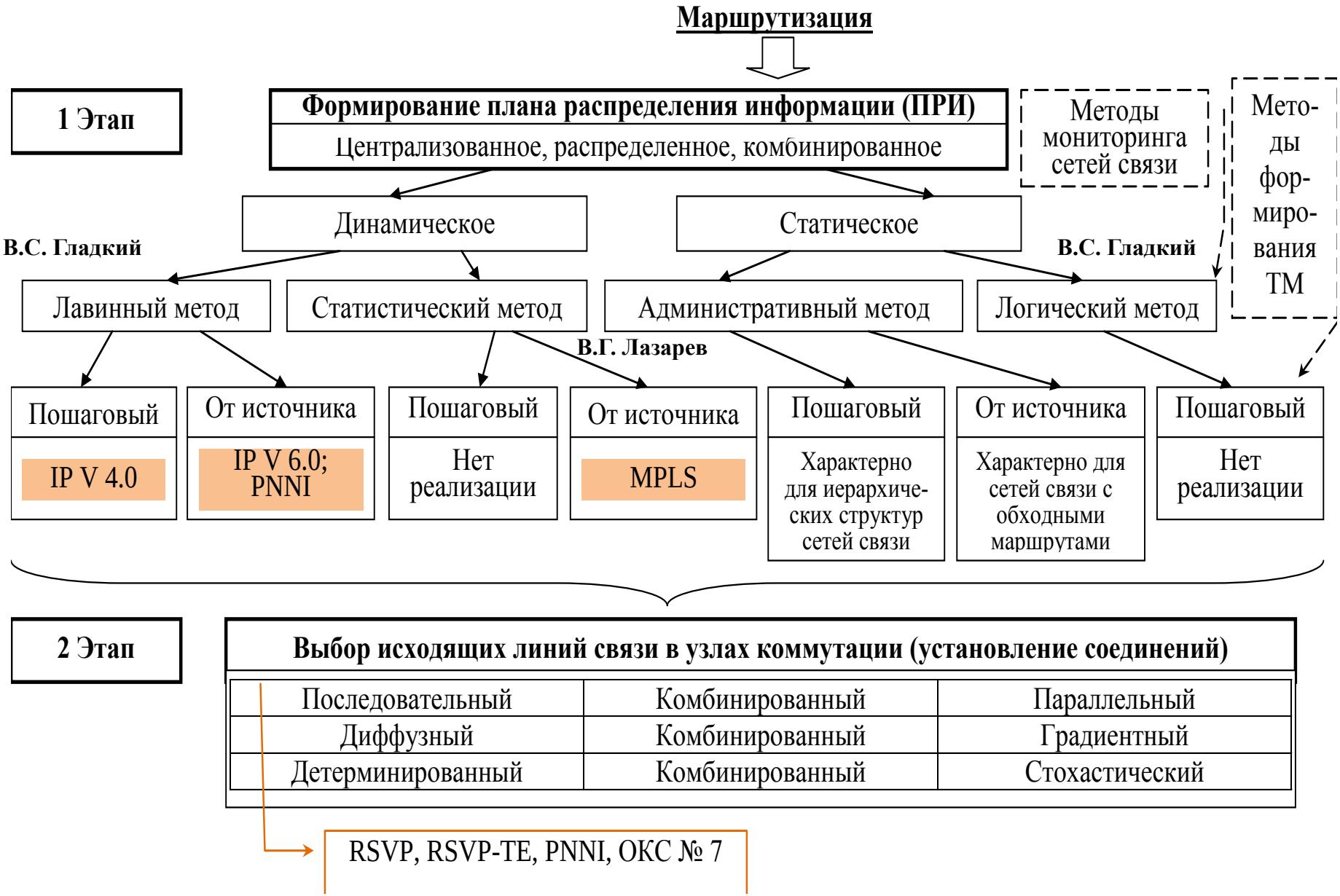
Необходимость в разработке, исследовании новых **ММ**, способных решать задачи защиты информации с поддержкой QoS приложений МСС

Лазарев, В.Г. Интеллектуальные цифровые сети: Справочник /Под ред. Н.А. Кузнецова. – М.: Финансы и статистика, 1996. – 224 с.: ил.



Обобщенная, функциональная модель маршрутизации в МСС

Классификация методов маршрутизации в сетях связи



1. Математическая модель влияния методов формирования ПРИ на объем доступных сетевых ресурсов

2. Математическая модель маршрутизации в условиях входного самоподобного трафика и внешних деструктурирующих воздействий на элементы МСС

3. Методика определения ПРИ на однородной ячеистой сети связи большой размерности

4. Упрощенная имитационная модель маршрутизации методом статистического моделирования

ММ влияния методов формирования ПРИ на объем доступных сетевых ресурсов

$$R_{\text{ТМ}}^{(ROUT)} = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_1 \cdot x + a_0;$$

$a_i; i = \overline{0,n}$ – коэффициенты, значение которых зависит от применения метода маршрутизации на сети связи

$0 \le x \le 1$ – переменная, которая определяет степень недоступности сетевых ресурсов МСС

$$R_{\text{ТМ}}^{(\text{лав})} = a_0 = \frac{K \cdot B \cdot S}{\Delta t}$$

$$R_{\text{П}}^{(\text{лав})} = (1 - x) - \frac{K \cdot B \cdot S}{\Delta t \cdot R_{\text{О}}} = 1 - x - y$$

$$R_{\text{П}}^{(\text{стат})} = (1 - x) - \frac{\left(a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0\right)}{R_{\text{О}}} = 1 - x - a'^{(\text{стат})}_0 - \sum_{i=1}^{n} a'^{(\text{стат})}_i$$

$$R_{\text{П}}^{(\text{стат})} \le 1 - x - a'_1 \cdot x$$

$$P_{\varepsilon(L)}^{(ROUT)} = \left\| p_{\varepsilon(L)i}^{(ROUT)\,j} \right\|_{S,S} \; i, j = \overline{1,S};$$

$$\lambda_{\text{o}\,i}^{(ROUT)\,j} = \sum_{L=1}^{S} \sum_{\varepsilon=1}^{\text{E}} \lambda_{\varepsilon} \cdot \pi_{\varepsilon,i,j} \cdot p_{\varepsilon(L)i}^{(ROUT)\,j}; i, j = \overline{1,S}; i \neq j;$$

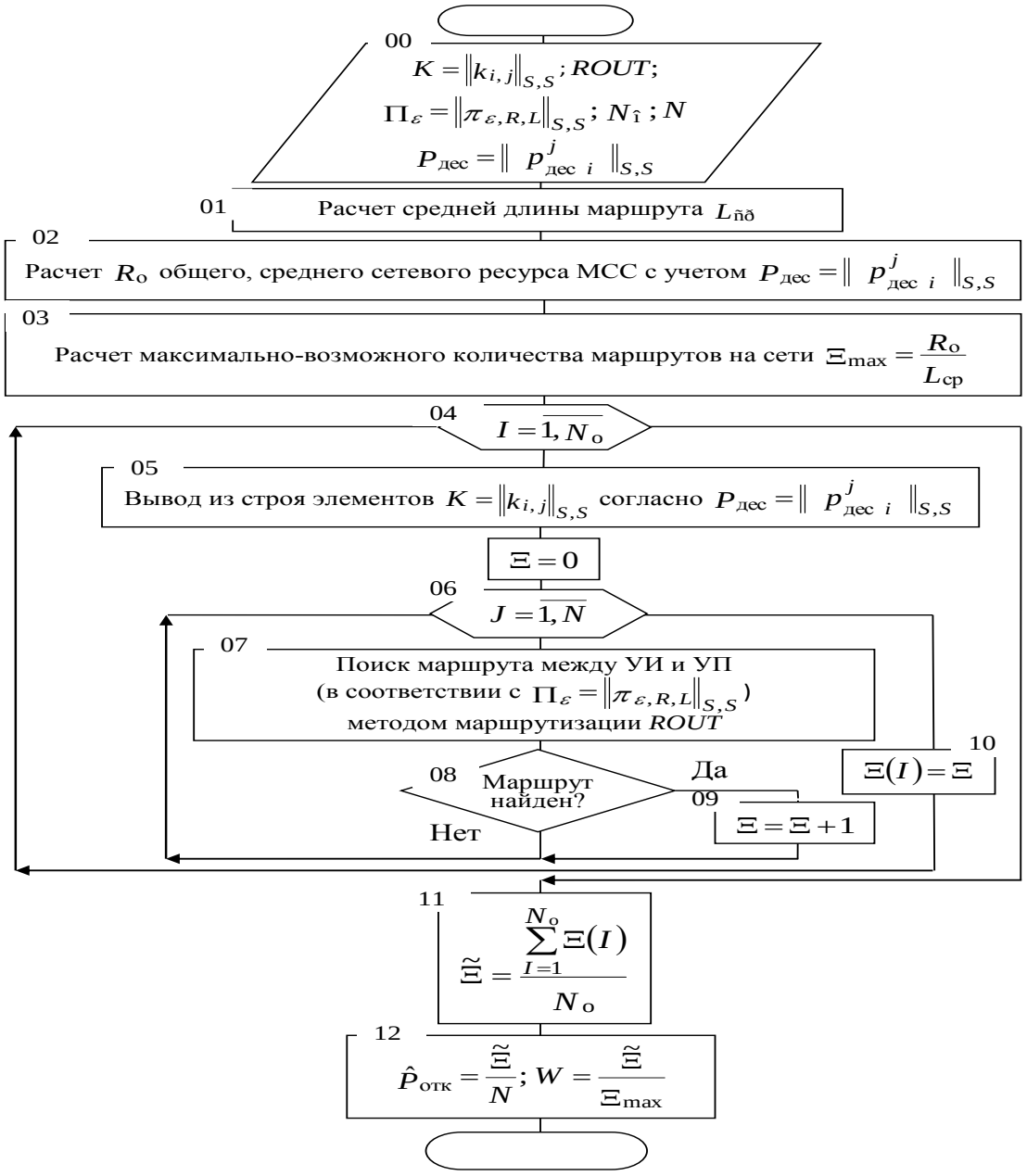
$$p_{\text{отк}\;i}^{(ROUT)\,j} = \int_{x_{\text{отк}}}^{\infty} \left[\frac{\lambda_{\text{o}\,i}^{(ROUT)} H_{\max} j \cdot x H_{\max}{}^{-1} \cdot e^{-\lambda_{\text{o}\,i}^{(ROUT)\,j \cdot x}}}{\int_{0}^{\infty} x H_{\max}{}^{-1} \cdot e^{-x} dx} - \mu_{ij} e^{-\mu_{ij} \cdot x} \right] dx; i, j = \overline{1,S}; i \neq j;$$

$$P_{\text{над}\;i}^{j} = (1 - p_{\text{отк}\;i}^{(ROUT)\,j}) \cdot (1 - p_{\text{дес}\;i}^{j}); i, j = \overline{1,S; i \neq j};$$

$$\hat{p}_{\text{отк}}^{(R,L)} = 1 - \sum_{k=1}^{2^{\kappa}} Q_{RJ}^{(k)} \cdot p_k = 1 - \sum_{k=1}^{2^{\kappa}} Q_{RL}^{(k)} \cdot \left(\prod_{\varphi=1}^{\kappa} p_{\varphi}^{\sigma_{\varphi}} \cdot q_{\varphi}^{1-\sigma_{\varphi}} \right); R, L = \overline{1,S};$$

$$\hat{P}_{\text{отк}} = 1 - \sum_{k=1}^{2^{\kappa}} Q_{o}^{(k)} \cdot p_k = 1 - \sum_{k=1}^{2^{\kappa}} Q_{o}^{(k)} \prod_{\varphi=1}^{\kappa} p_{\varphi}^{\sigma_{\varphi}} \cdot q_{\varphi}^{1-\sigma_{\varphi}}.$$

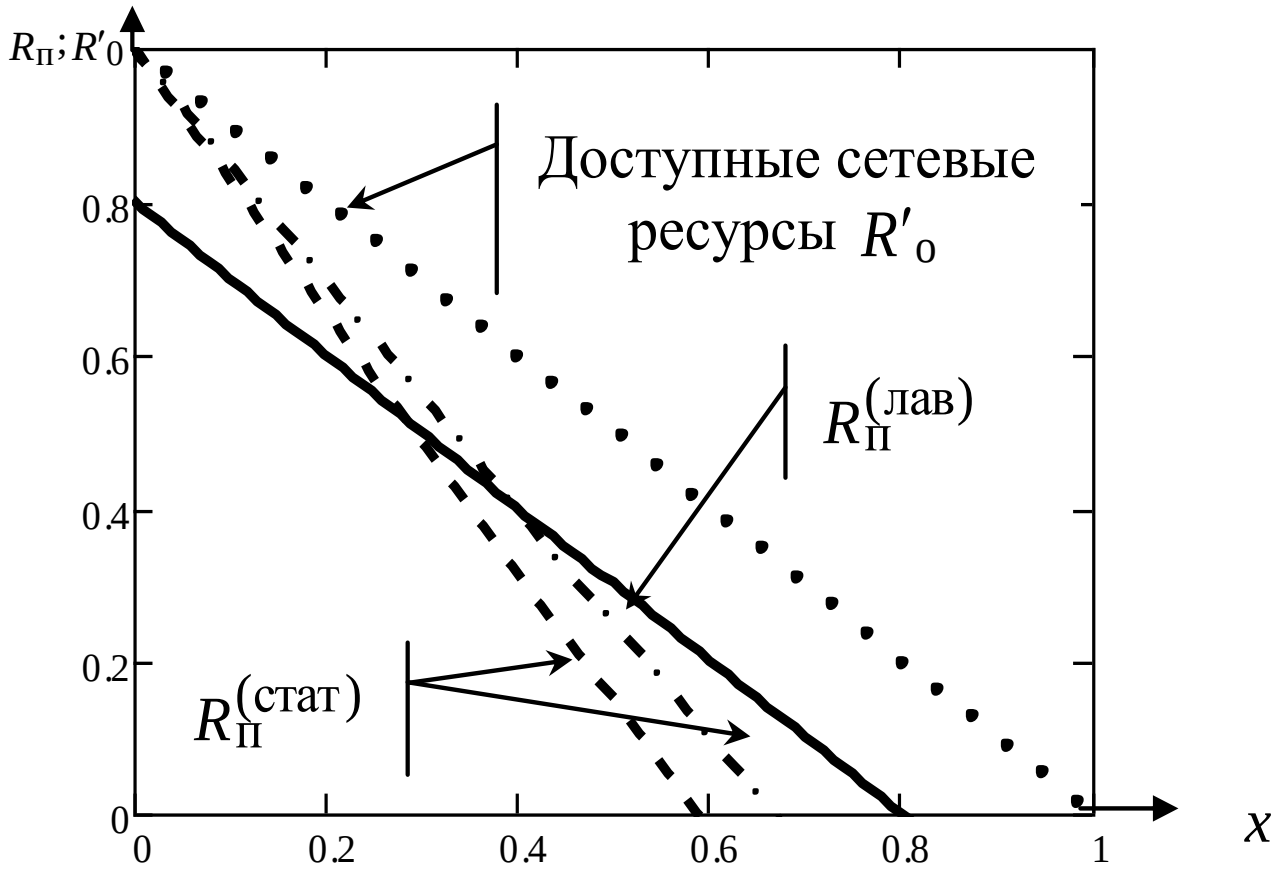
Упрощенная имитационная модель маршрутизации методом статистического моделирования



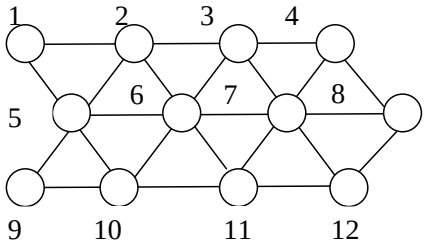
$$\hat{P}_{\text{отк}} = \frac{\tilde{\Xi}}{N},$$

$$W = \frac{\tilde{\Xi}}{\Xi_{\max}}$$

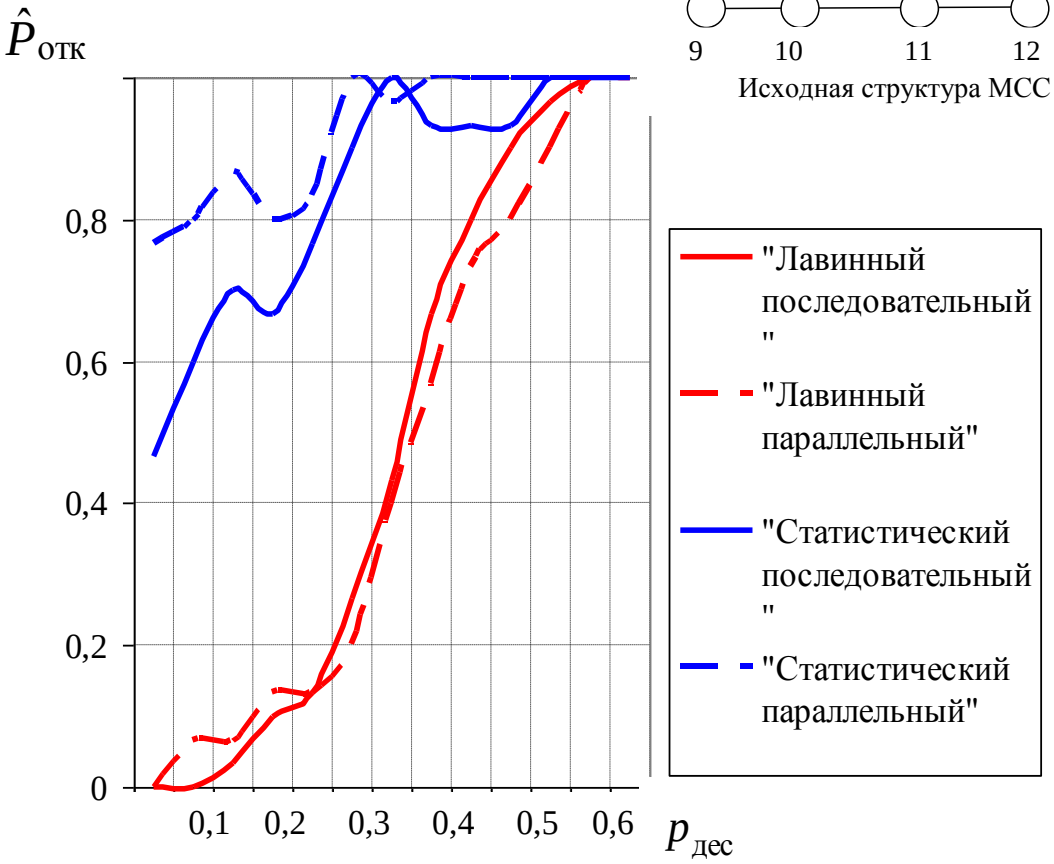
Графики зависимостей $R_{\text{П}}^{(\text{лав})}$, $R_{\text{П}}^{(\text{стат})}$



Результаты математического моделирования маршрутизации в условиях входного самоподобного трафика и внешних деструктурирующих воздействий на элементы МСС



Исходная структура МСС



Зависимости вероятности отказа в обслуживании в целом по МСС при $\lambda_1 = 10 \cdot 10^6$

1. Пропускная способность ТПС

$$\mu = \mu_{ij} = 100 \cdot 10^6; i, j = \overline{1,12}; i \neq j$$ пакетов/сек

2. Длительность обслуживания пакетов сообщений, поступающего асинхронного потока данных в ТПС УК подчияется экспоненциальному закону с параметром $w = \frac{1}{\mu}$

3. Интенсивность поступления пактов в МСС $\lambda = \lambda_\varepsilon; \varepsilon = \overline{1,E}; \quad \lambda_1 = 10 \cdot 10^6; \quad \lambda_2 = 50 \cdot 10^6$

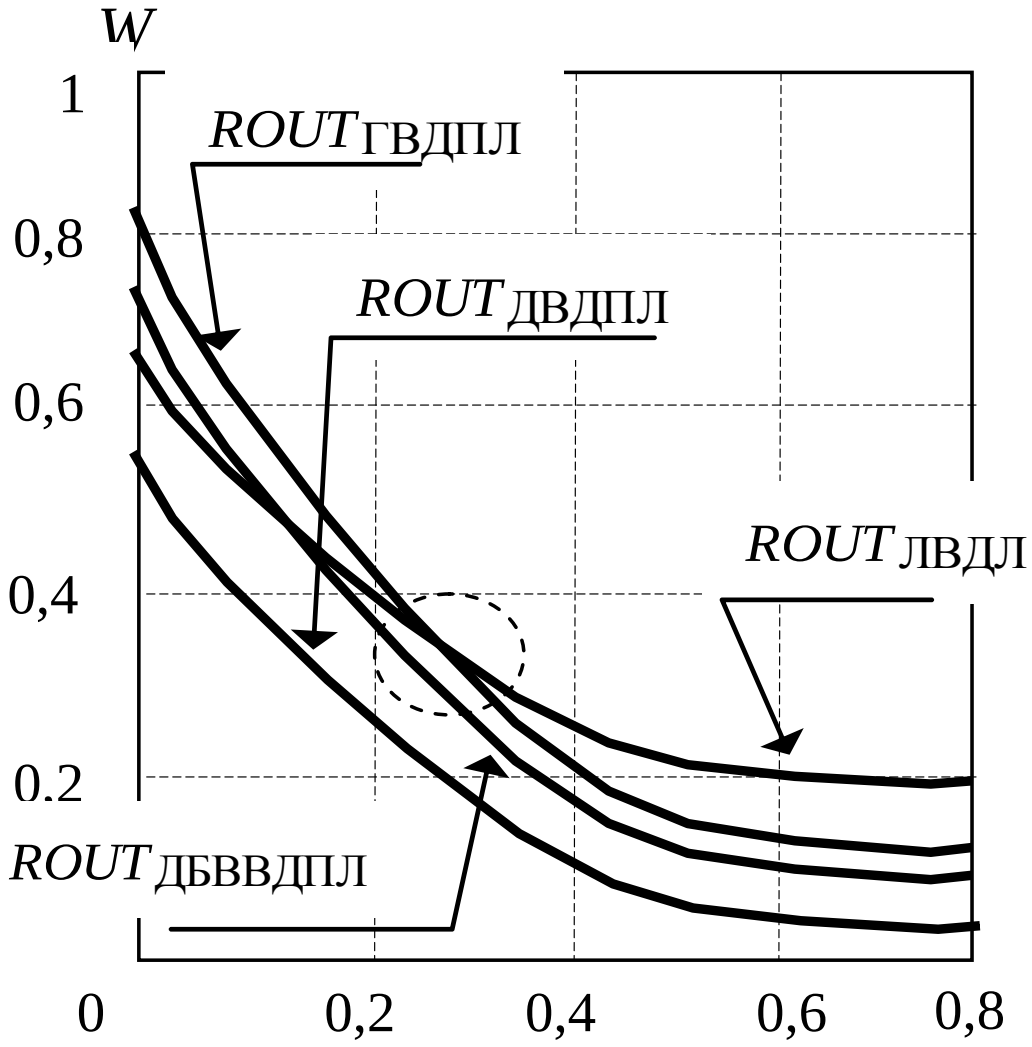
4. $H = H_\varepsilon = 0{,}5; \quad \varepsilon = \overline{1,E}$

5. $\Pi_\varepsilon = \left\| \pi_{\varepsilon,R,L} \right\|_{S,S};$

$$0 \le \pi_{\varepsilon,R,L} \le 1; \sum_{R,N=1}^{S} \pi_{\varepsilon,R,L} = 1; \varepsilon = \overline{1,E}$$

6. $P_{дес} = \| \; p^j_{дес\ i} \; \|_{S,S},$

Результаты статистического моделирования маршрутизации на упрощенной имитационной модели сети связи



$$W = f(P_{\text{отк}})$$

для различных методов маршрутизации

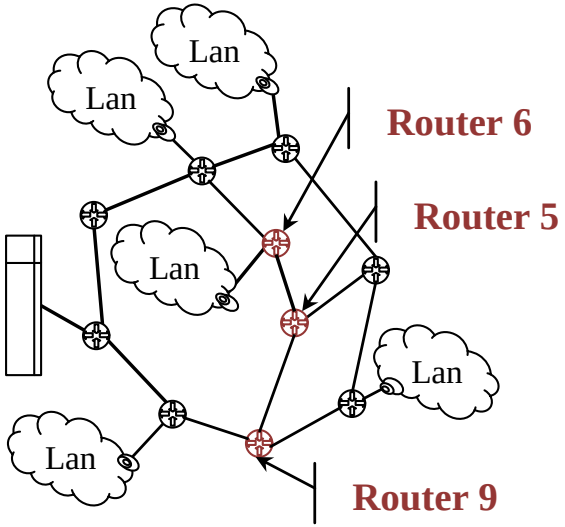
$$S = X_{\max} \cdot Y_{\max} = 50$$

$$k_{i,j} = 8; i, j = \overline{1,50};$$

$$p_{\text{дес}} = p^{j}_{\text{дес } i}; i, j = \overline{1,S}$$

$$\pi_{i,j} = \frac{1}{S^2}; i, j = \overline{1,S}$$

$$N_{\text{o}} = 1000$$



Структура анализируемой МСС

с 0 по 5 минуту моделирования

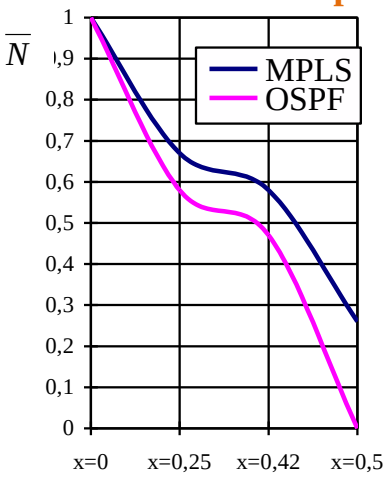
Порядок выхода маршрутизаторов из строя

$$\overline{N} = 1 - \frac{N_{\text{потерь}}^{(j)}}{N_{\text{потерь}}(\max)};\ j = \overline{1,3}$$

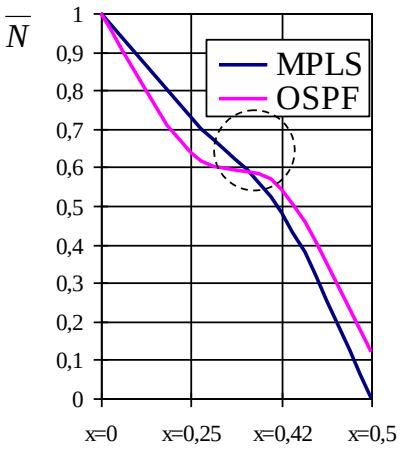
$$x_i = \frac{R_0 - R_0^{(i)}}{R_0};\ i = \overline{1,4}$$

$$\begin{cases} R_0^{(1)} = 12 \cdot r & \text{интервал моделирования } 0 \div 5 \text{ минут;} \\ R_0^{(2)} = 9 \cdot r & \text{интервал моделирования } 5 \div 10 \text{ минут;} \\ R_0^{(3)} = 7 \cdot r & \text{интервал моделирования } 10 \div 15 \text{ минут;} \\ R_0^{(4)} = 6 \cdot r & \text{интервал моделирования } 15 \div 30 \text{ минут.} \end{cases}$$

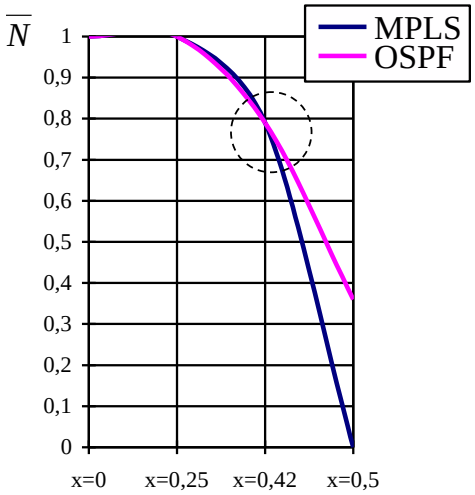
Мрезультаты моделирования МСС в условиях ограниченных сетевых ресурсов с использованием Opnet Modeler v 14.0.



Нормированные результаты моделирования при r = 1000 Мбит/с



Нормированные результаты моделирования при r = 100 Мбит/с



Нормированные результаты моделирования при r = 10 Мбит/с

Выводы

1. При условии выхода из строя более 20 % - 30 % сетевых ресурсов МСС «Лавинные параллельные» методы маршрутизации по сравнению со «Статистическими» показывают лучшие результаты.

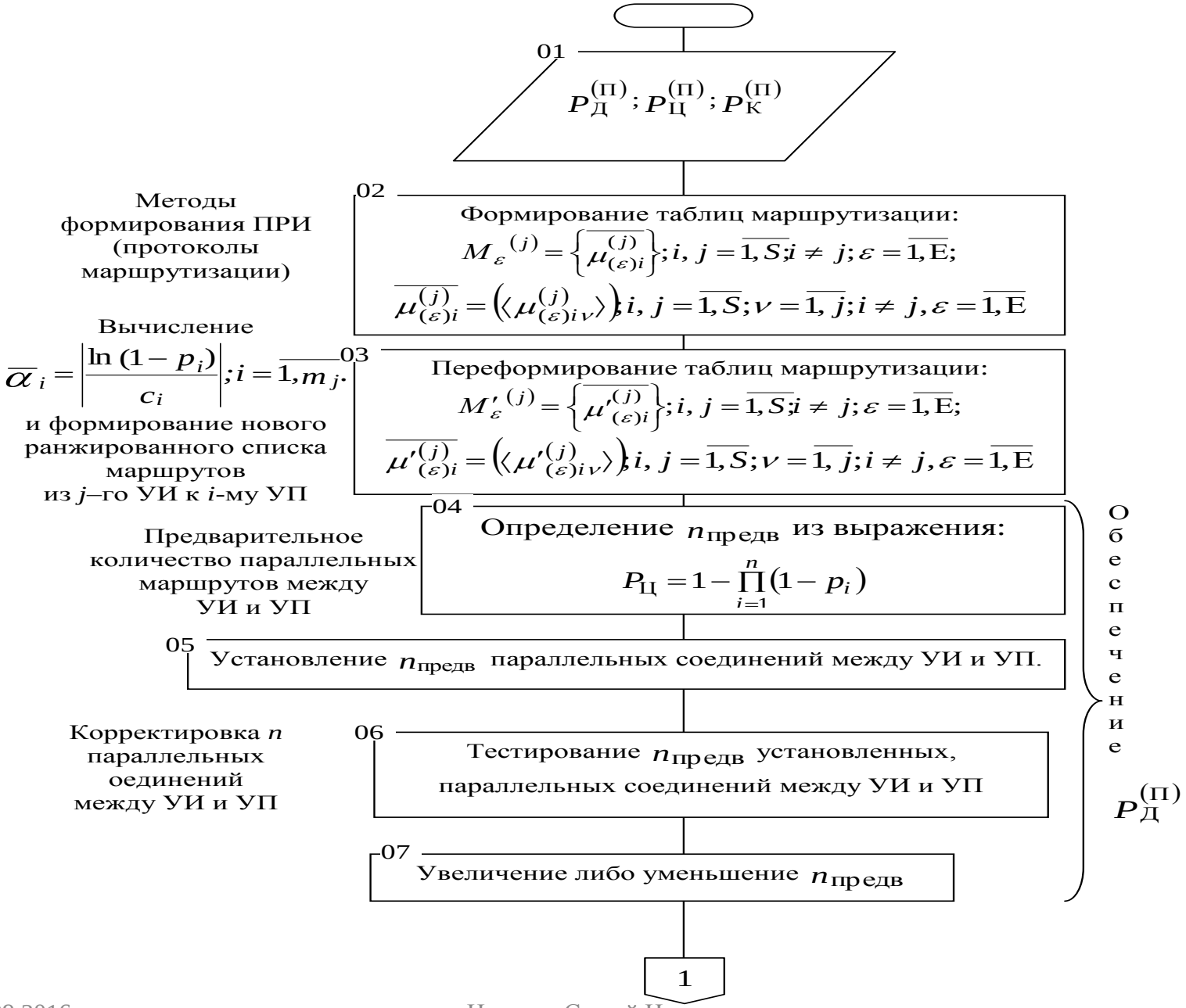
Данный результат независимо подтвержден на различных структурах МСС и с применением различных математических и имитационных моделей.

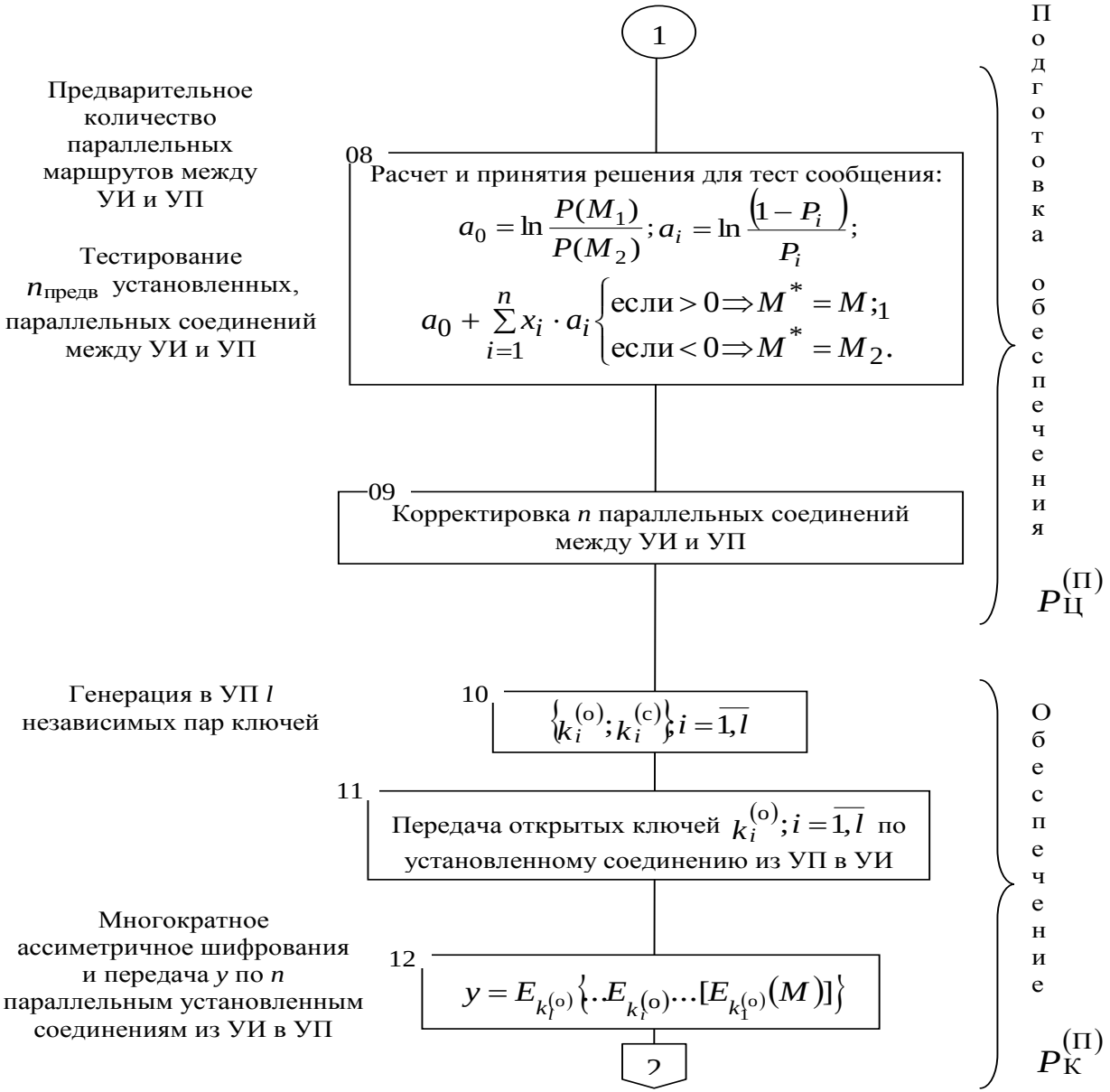
2. Резервирование сетевых ресурсов на этапе проектирования МСС более 30% позволит:

- в условиях внешних деструктивных воздействий на элементы МСС увеличить возможность передачи большего объема пользовательской информации;

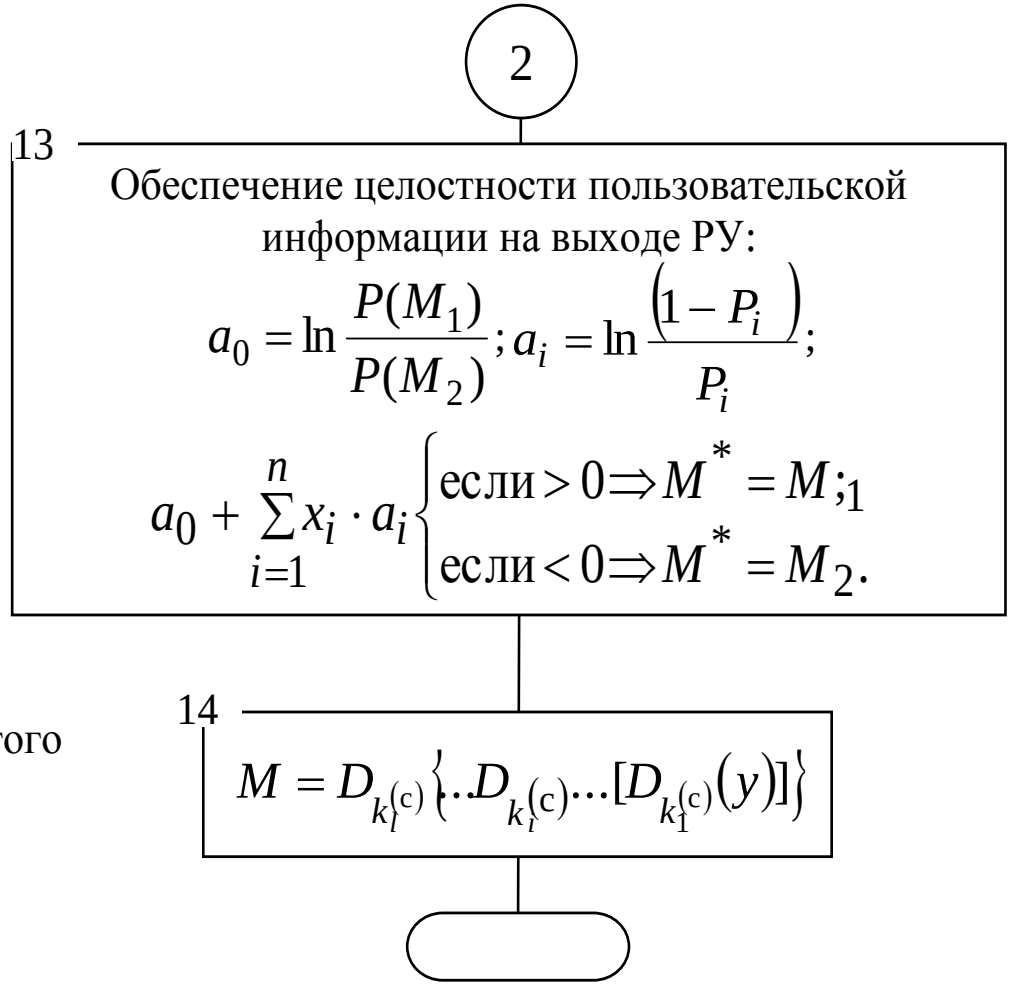
- реализовать защиту информации (конфиденциальность, доступность и целостность) за счет **ММ** путем использования территориально-распределенных ресурсов в МСС (каналов связи, криптографических программно-аппаратных комплексов, баз данных и т. п.).

Методики защиты информации за счет сетевых ресурсов МСС




1
Предварительное количество параллельных маршрутов между УИ и УП
Тестирование $n_{предв}$ установленных, параллельных соединений между УИ и УП
08
Расчет и принятия решения для тест сообщения:
$a_0 = \ln \frac{P(M_1)}{P(M_2)}; a_i = \ln \frac{(1-P_i)}{P_i};$
$a_0 + \sum_{i=1}^{n} x_i \cdot a_i$ если $>0 \Rightarrow M^* = M;_1$ если $<0 \Rightarrow M^* = M_2.$
09
Корректировка n параллельных соединений между УИ и УП
Подготовка обеспечения $P_Ц^{(П)}$
Генерация в УП l независимых пар ключей
10
$\{k_i^{(о)}; k_i^{(с)}\}; i = \overline{1,l}$
11
Передача открытых ключей $k_i^{(о)}; i = \overline{1,l}$ по установленному соединению из УП в УИ
Многократное ассиметричное шифрования и передача y по n параллельным установленным соединениям из УИ в УП
12
$y = E_{k_l^{(о)}}\{..E_{k_i^{(о)}}...[E_{k_1^{(о)}}(M)]\}$
2
Обеспечение $P_К^{(П)}$

Передача пользовательской информации ε-го приложения МСС по n параллельным соединениям между УИ и УП



Расшифрование в УП принятого сообщения

Выполненные в работе научные исследования представлены следующими новыми результатами

1. *Разработана методология*, основанная на протоколах сетевого уровня МСС, которая позволяет обеспечить базовые параметры ИБ (конфиденциальность, доступность, целостность).

2. *Предложен подход* к обеспечению конфиденциальностм информации, использующий многократное асимметричное шифрование ключами меньшей длины позволяет уменьшить время шифрования в l^{c-1} раз, где l – количество асимметричных шифрований, – постоянная, значение которой определяется криптографическими алгоритмами шифрования.

3. *Предложен критерий*, позволяющий выбирать маршруты с точки зрения обеспечения целостности и доступности передаваемой информации в мультисервисных сетях связи при минимальной стоимости.

4. *Разработаны способ и алгоритм*, отличающиеся тем, что для обеспечения целостности информации используют параллельные (многопутевые) методы маршрутизации, что позволяет уменьшить время задержки передачи информации.

5. *Разработан алгоритм* обеспечения доступности информации в МСС, отличающийся тем, что между УИ и УП устанавливают параллельные соединения, обеспечивающие вероятностно-стоимостные параметры.

6. *Предложена новая классификация ММ*, отличающаяся наличием независимых процедур − формированием плана распределения информации на сети и выбором исходящих трактов передачи информации в узлах коммутации, что позволяет: выявить новые методы маршрутизации; провести целенаправленный анализ и синтез методов маршрутизации, которые будут эффективно функционировать в условиях штатной эксплуатации и внешних деструктивных воздействий на элементы мультисервисной сети связи.

7. *Предложен новый метод маршрутизации* («Гибридный»), отличающийся тем, что в зависимости от степени воздействия внешних деструктивных факторов на мультисервисную сеть связи, используют «Логический», «Статистический» или «Лавинный» методы, что позволяет сократить объем передаваемой служебной информации в мультисервисной сети связи во время ввода узлов коммутации в эксплуатацию, штатной эксплуатации и в условиях внешних деструктивных воздействий на элементы сети.

8. *Разработан инструментарий* (методики, модели, алгоритмы, программные продукты) позволяющий проводить анализ методов маршрутизации в МСС и включающий в себя:

- математическую модель для оценки влияния методов формирования плана распределения информации на объем сетевых ресурсов;
- математическую модель маршрутизации в условиях входного самоподобного трафика и внешних деструктивных воздействий на элементы МСС;
- методики определения плана распределения информации на однородной ячеистой сети связи большой размерности;
- упрощенную имитационную модель маршрутизации;
- способ проверки графа сети на связность, отличающийся тем, что анализируемый граф «разбивают» на подграфы; каждый подграф проверяют на связность «стягиванием» смежных вершин, к первоначально выбранной, до тех пор, пока подграф не представится в виде одиночной точки или множества точек; в результате формируется суперграф, который проверяется на связность «стягиванием» смежных вершин, к первоначально выбранной, до тех пор, пока суперграф не представится в виде одиночной точки (исходный граф связен) или множества точек (исходный граф не связен); это позволяет уменьшить алгоритмическую сложность решения задачи в $\sqrt{S}$ (S – количество вершин графа) по сравнению с известными способами.

9. Проведен анализ функционирования МСС в условиях внешних деструктивных воздействий, который показал (усредненные данные), что в случае выхода из строя более 30% элементов МСС параллельные (многопутевые) методы маршрутизации позволяют понизить до 20% среднюю вероятность отказа заявок пользователей на обслуживание.

10. Разработан инструментарий (методики, методы, алгоритмы), позволяющий за счет применения новых методов маршрутизации, реализовать защиту информации с обеспечением показателей качества обслуживания приложений МСС.

Представленные подходы к защите информации являются перспективными для реализации параметров информационной безопасности, представленных в ITU-T Recommendation X.805 Security Architecture for Systems providing end-to-end Communications.

Особое внимание представляет развитие исследований и разработок, которые могли бы быть использованы в программно-конфигурируемых сетях

(SDN, Software-defined Networking)

Всего по данной тематике опубликовано **90** работ в том числе:

- **18** статей в научных журналах и изданиях, рекомендованных ВАК РФ;
- **патент** на способ изобретения;
- **10** свидетельств на программы для ЭВМ, зарегистрированных в установленном порядке;
- **8** работ, включенных в библиографические базы Web of Science и Scopus;
- **2** рецензируемых монографии;
- **4** рецензируемых учебных пособия с грифом УМО;

Защищено 2 к.т.н. и подготовлена д.т.н.

Благодарю за внимание!