МОДЕЛИ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МУЛЬТИСЕРВИСНЫХ СИСТЕМАХ СВЯЗИ НА ОСНОВЕ НЕЧЁТКИХ СИТУАЦИОННЫХ СЕТЕЙ

С. А. Агеев, И.Б. Саенко

ОАО «Радиоавионика», Военная академия связи, Санкт-Петербург

АКТУАЛЬНОСТЬ ПРОБЛЕМЫ:

- Возрастающие требования к качеству функционирования МСС;
- Обеспечения информационной безопасности как передаваемого контента, так и самой информационной инфраструктуры МСС;
- Необходимость оперативного реагирования АСУС МСС на возникающие риски угроз ИБ МСС.

ЦЕЛЬ РАБОТЫ :

- Повышение оперативности реагирования системы на повышение уровня рисков угроз ИБ МСС;
- Повышение достоверности и обоснованности принимаемых управленческих решений по управлению рисками угроз ИБ МСС.

Мультисервисные сети связи (МСС) как объект управления

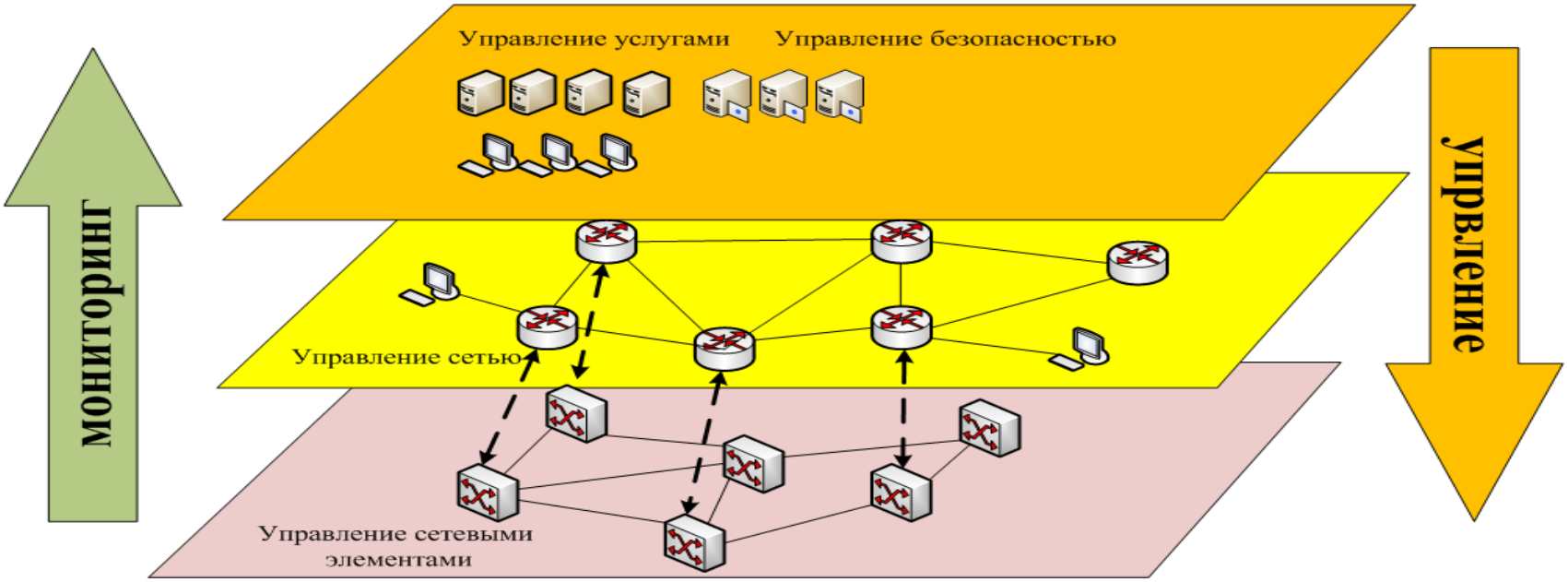


Рис.1 Функциональные уровни управления МСС

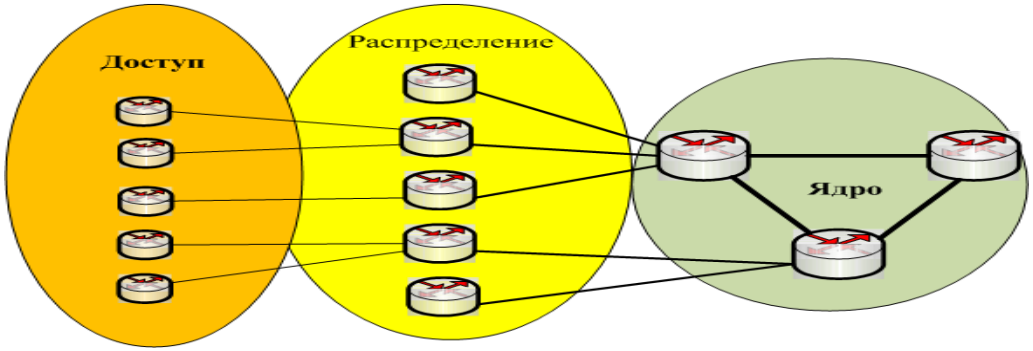


Рис.2 Составляющие компоненты МСС

МСС создаётся на принципах создания сетей NGN

Составляющие цикла управления рисками угроз ИБ МСС

$$P_{oy} = P(t_y \le T_{zy})$$

$$t_y = t_{cб} + t_a + t_p + t_д + t_u + t_n$$

Poy – вероятность события заключающегося в том, что время цикла управления не превысит заданное время ***Tзy***;
tcб - время сбора информации о состоянии сетевых элементов, поступающей от подсистемы сетевого мониторинга;
ta - время анализа информации;
tp - время выработки решений;
tд - время доведения управляющей информации до соответствующих сетевых элементов;
tu - время реализации сетевыми элементами управленческих решений ;
tn - время подтверждения сетевыми элементами выполнения управленческих решений.

Модификация иерархической структуры модели *TMN* для МСС

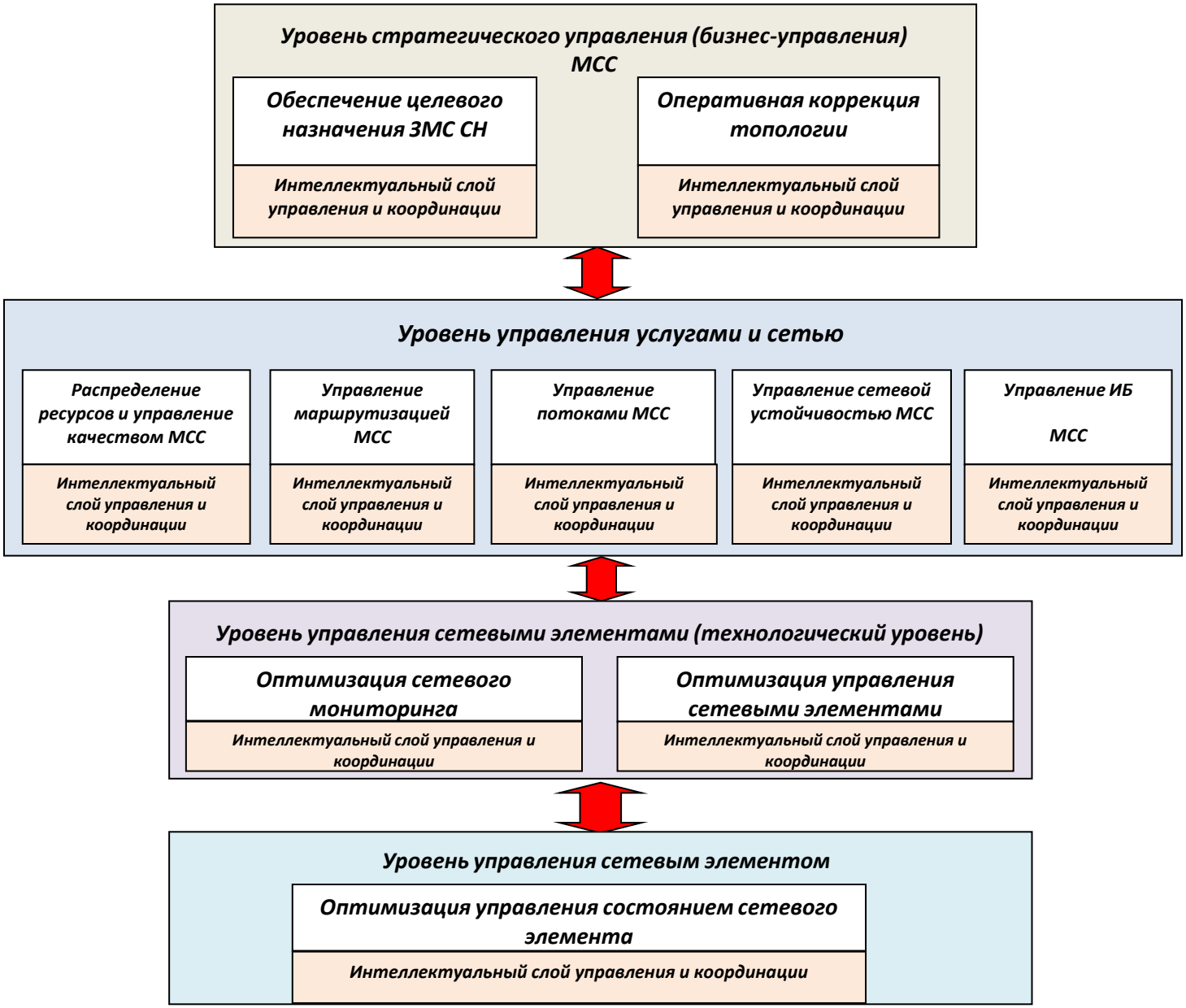
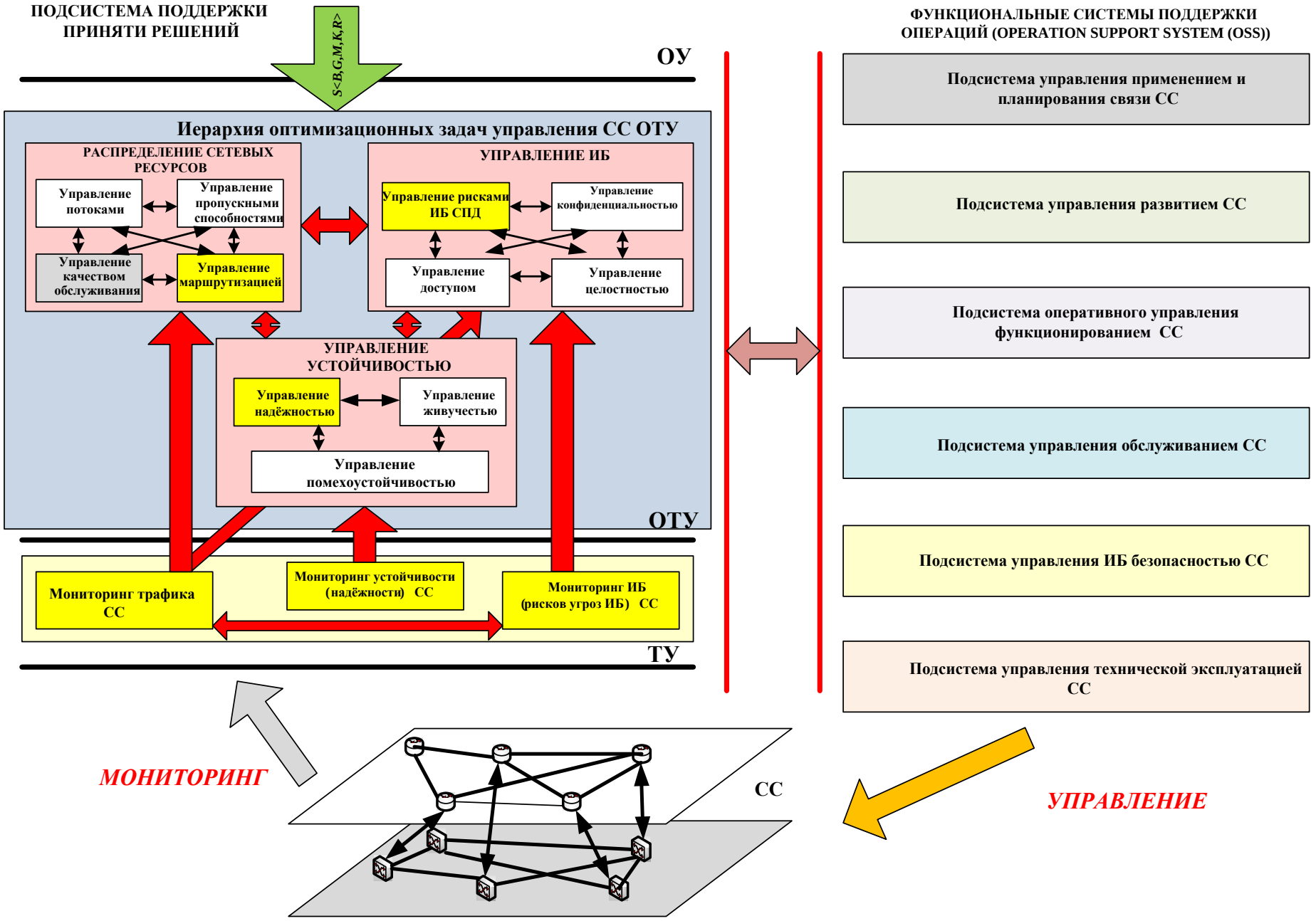
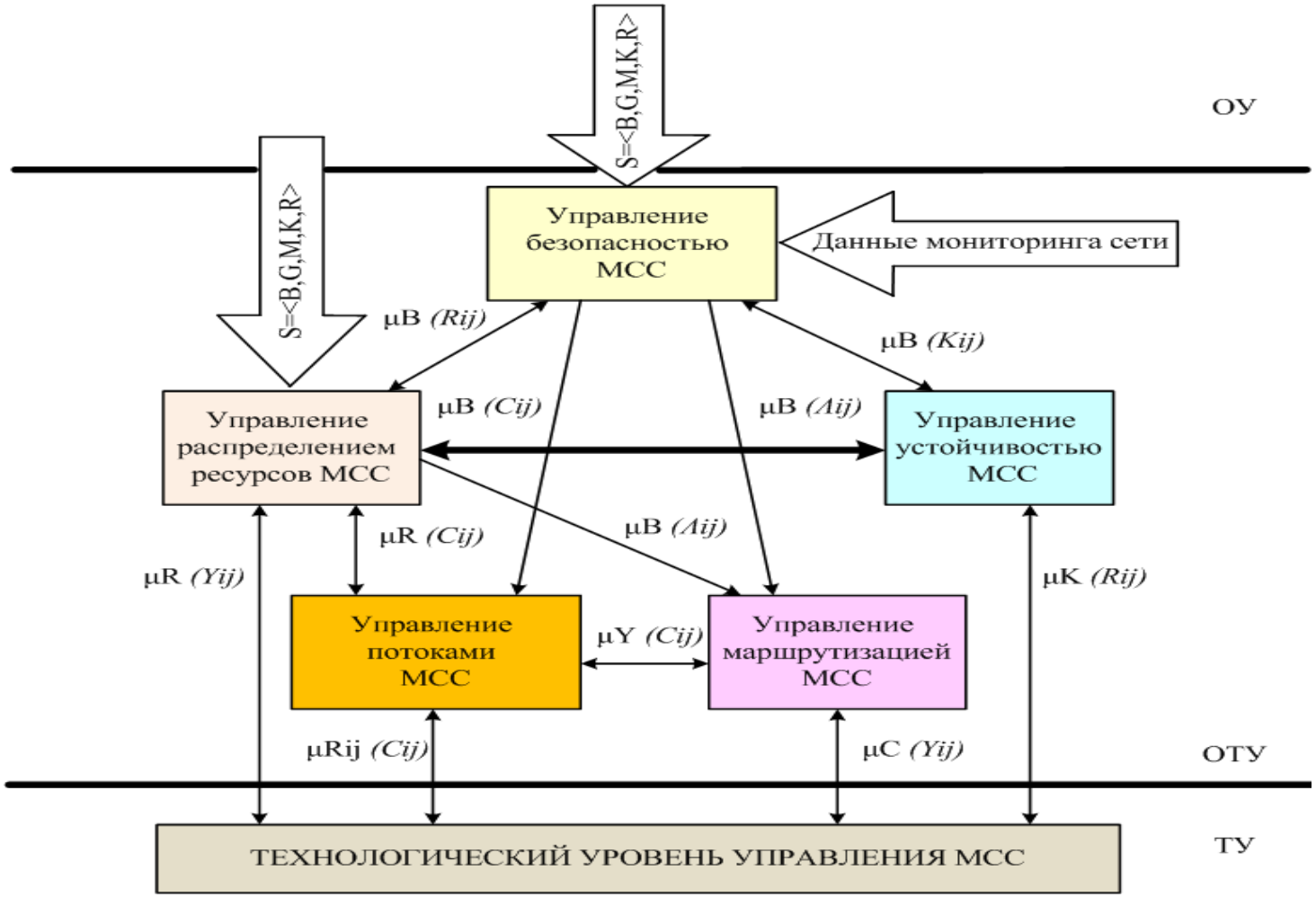


Схема потоков задач автоматизированного управления МСС



Взаимодействие задач управления МСС на основе метода нечёткой координации решений (принцип Беллмана – Заде)



μ<*> -функция принадлежности вектора управляющих параметров, ***S<B,G,M,K,R>*** - требуемое состояние МСС, где: ***B*** – состояние ИБ МСС, ***G*** – топология МСС, ***M*** – число видов телематических услуг связи, KR_i – требуемое качество для ***i***–й услуги, R_i – требуемый телекоммуникационный ресурс для ***i***–й услуги связи, ***Cij***-пропускная способность каналов связи, ***Yij*** - виды услуг связи, ***Λij*** - интенсивность трафика, ***Kij*** - коэффициент исправного действия

Метод формирования управляющих решений на основе нечетких иерархических ситуационных сетей

G =(***S,R,α***) – нечеткий ориентированный взвешенный граф

S-эталонные нечеткие ситуации

R=(R1 … Rd)-возможные управляющие решения

α(Si, Rj) – степень предпочтения применения управляющего решения Rj в ситуации Si

Пример: $\hat{S}_к$ {((0,1/ низкая), (0,7/ средняя), (0,8/высокая)/надежность КС),
((0,8/ низкая), (0,4/ средняя), (0,1/высокая)/уровень риска угроз ИБКС),
((0,1/ низкая), (0,6/ средняя), (0,8/высокая)/ПС КС)}

Решение: Если S= $\hat{S}_к$, то предпочтительно ***Ri*** (использовать) КС -ПП

Метод нечёткого логического вывода Мамдани

Метод нечеткого логического вывода Мамдани:

$$\bigcup_{i=1}^{c}\left(\bigcup_{j=1}^{m} x_i = a_{i,j} \times w_j\right) \rightarrow y_j = d_j,\ j = \overline{1,m}$$

где X_i - набор входных признаков;

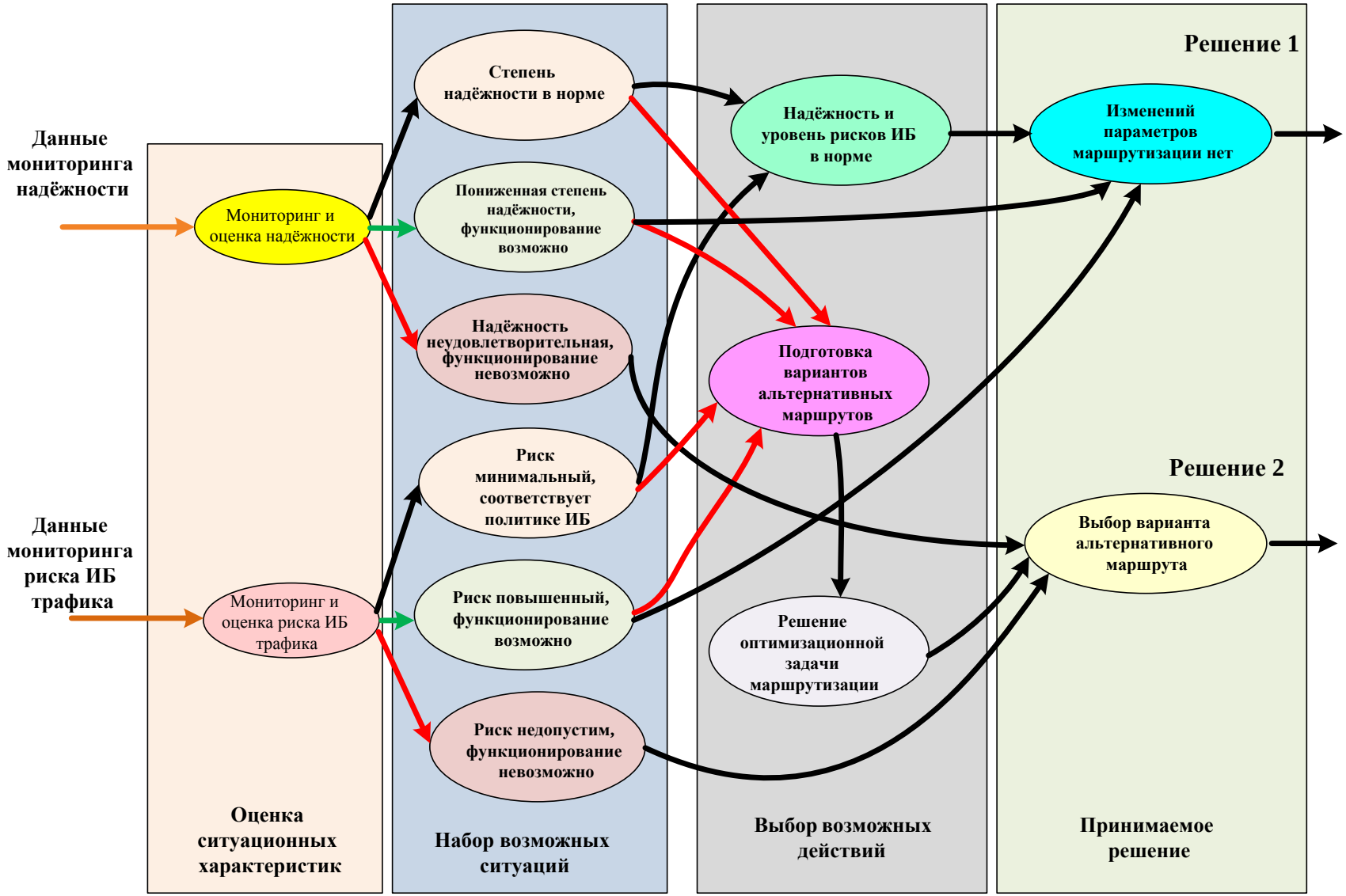
y_j - выходная переменная j-го правила;

$a_{i,j}$ -нечеткий терм, которым оценивается переменная в правиле j базы знаний ;

w_j -весовой коэффициент правила j;

d_j -набор значений выходной переменной.

ПРИМЕР РЕАЛИЗАЦИИ НСС



РАЦИОНАЛЬНОЕ РАСПРЕДЕЛЕНИЕ ПОТОКОВ

n – количество узлов коммутации;

M – количество каналов.

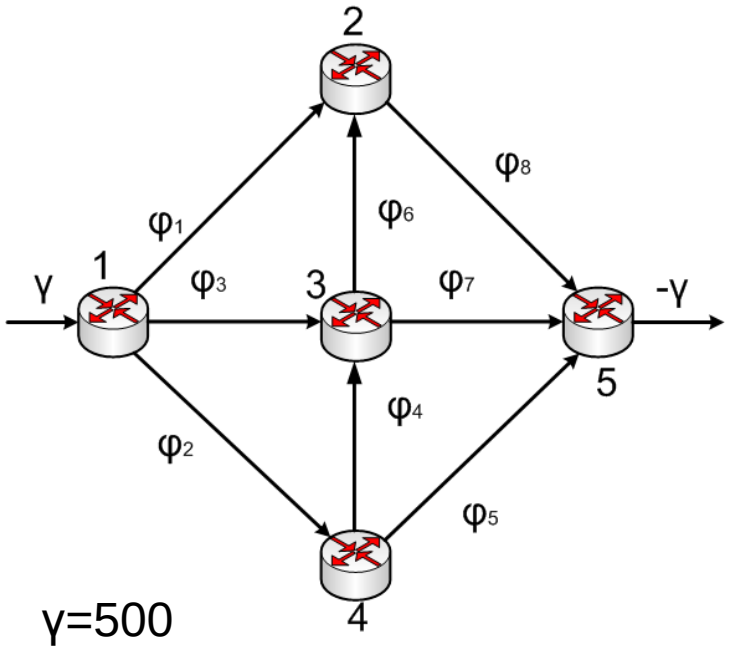
$$T = \frac{1}{\gamma}\sum_{i=1}^{M}\frac{f_i}{C_i - f_i} \times I(R_{ИБ}, H) \rightarrow \textbf{min};$$

где $I(R_{ИБ}, H)$ - индикаторная функция, зависящая от величины риска ИБ и от надёжности, которая вводится для координации решения задачи маршрутизации.

при выполнении ограничений:

$$0 \le f_i < C_i \; i = \overline{1, M};$$

$$\sum_{i \in E} f_i - \sum_{j \in E} f_j = \begin{cases} -\gamma, l = i; \\ 0, l \neq i; \\ \gamma, l = i \end{cases}$$ - условие сохранения потока



φ1	φ2	φ3	φ4	φ5	φ6	φ7	φ8
166.33	166.67	167	0.67	166.67	0.67	166.67	167
225	0.	275	75.5	199.5	-49.5	125	175.5

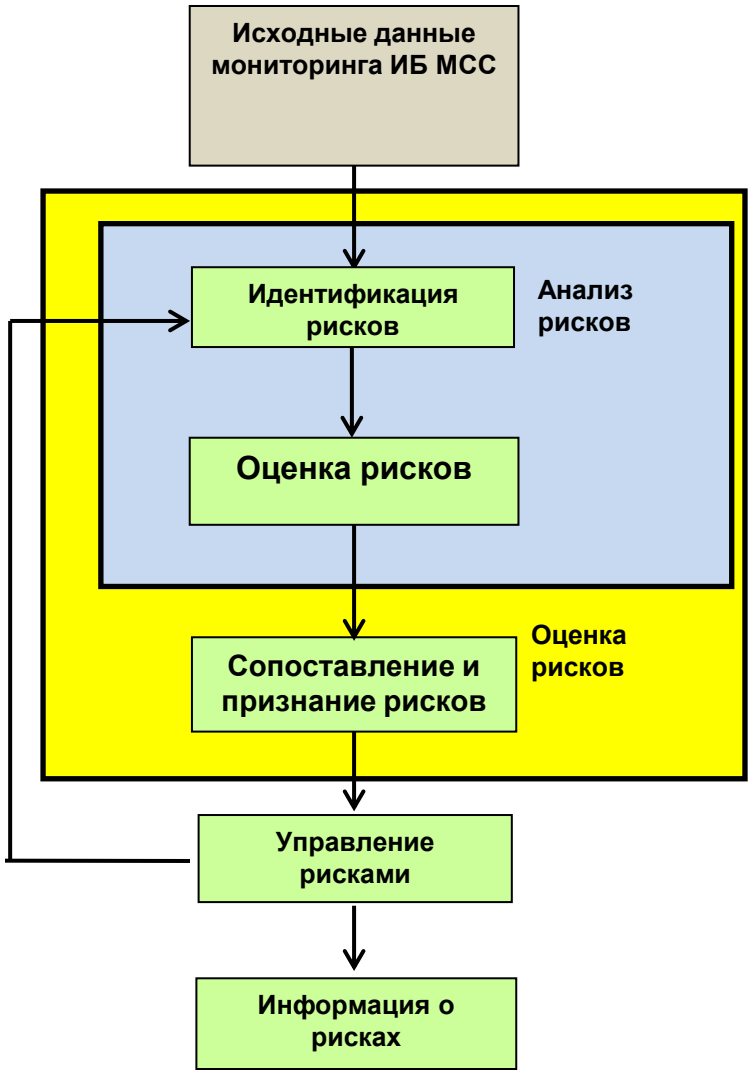
$C =$

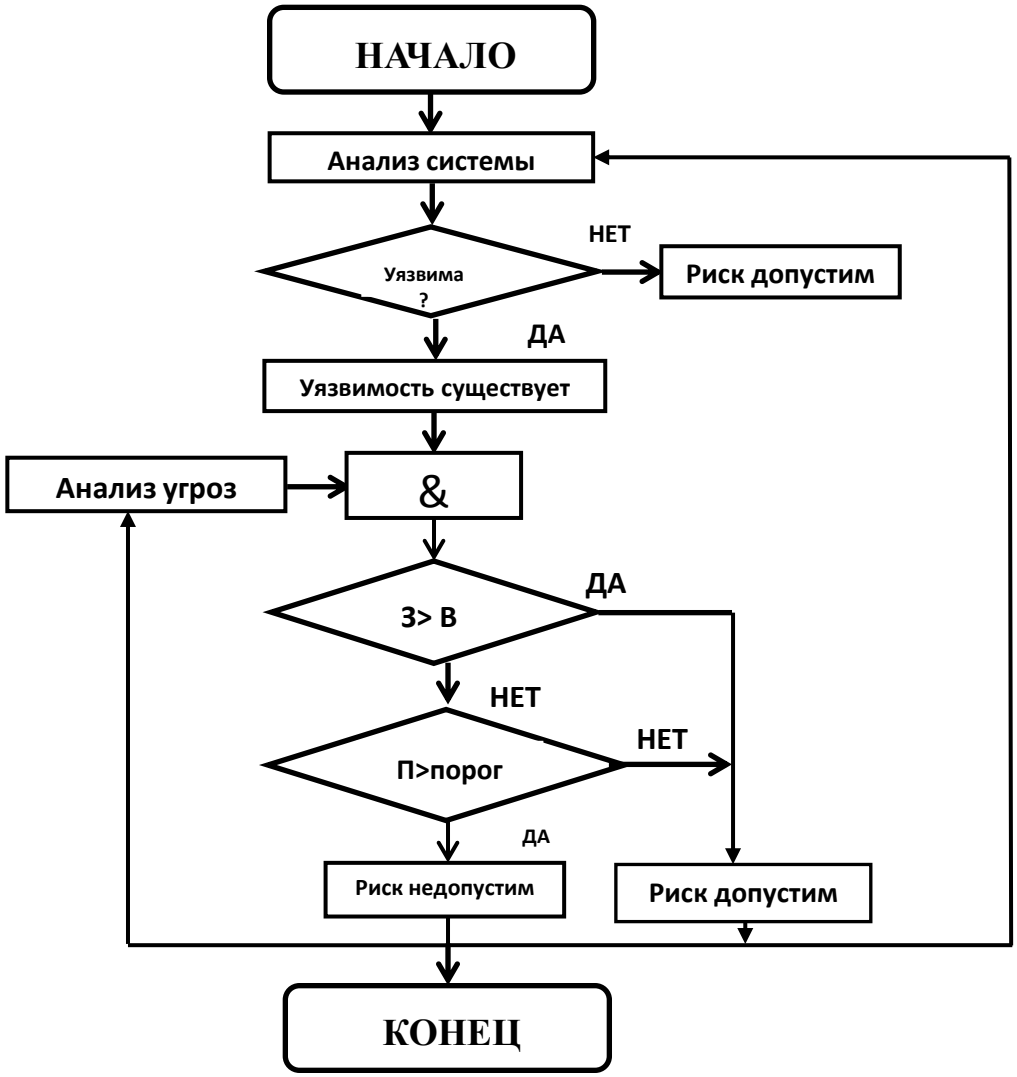
	1	2	3	4	5
1	0	250	250	200	0
2	250	0	200	0	200
3	250	200	0	250	200
4	200	0	250	0	250
5	0	200	200	250	0

Стандарты управления рисками ИБ МСС

<table>
<tr><th>Британский стандарт</th><th>Международный стандарт</th><th>Российский стандарт</th></tr>
<tr><td rowspan="2">BS 7799-1</td><td>ISO 27002: 2007</td><td>ГОСТ 17799: 2005</td></tr>
<tr><td colspan="2">ISO 17799: 2005</td></tr>
<tr><td>BS 7799: 2005</td><td>ISO 27001: 2005</td><td>ГОСТ 27001: 2005</td></tr>
<tr><td rowspan="2">BS 7799-3: 2006</td><td>Проект ISO 27005</td><td rowspan="2">ГОСТР ИСО/МЭК 27005-2010</td></tr>
<tr><td>ISO / IEC 27005:2011</td></tr>
</table>

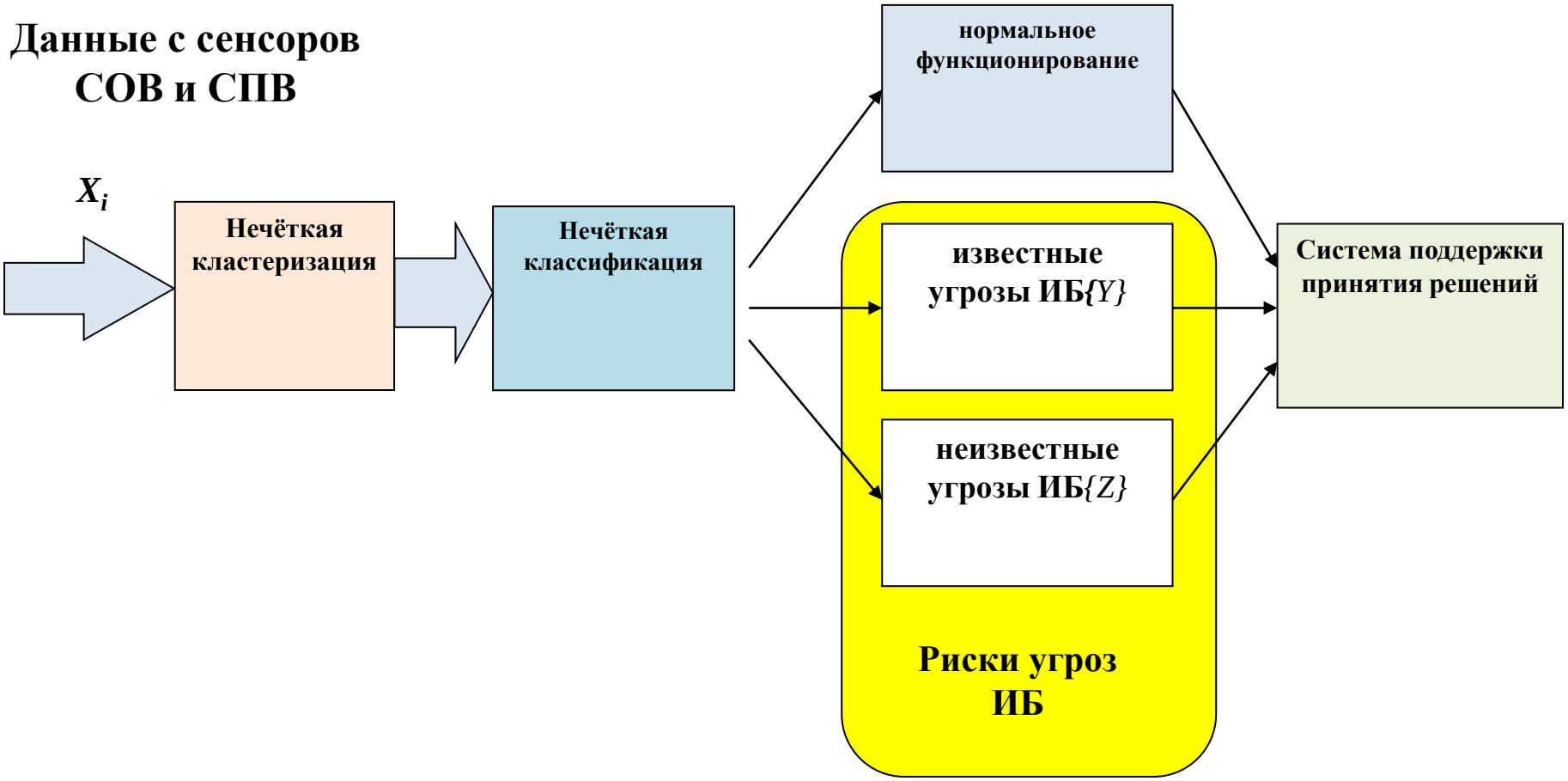
МЕТОДОЛОГИЯ И МЕТОД УПРАВЛЕНИЯ РИСКАМИ ИБ МСС



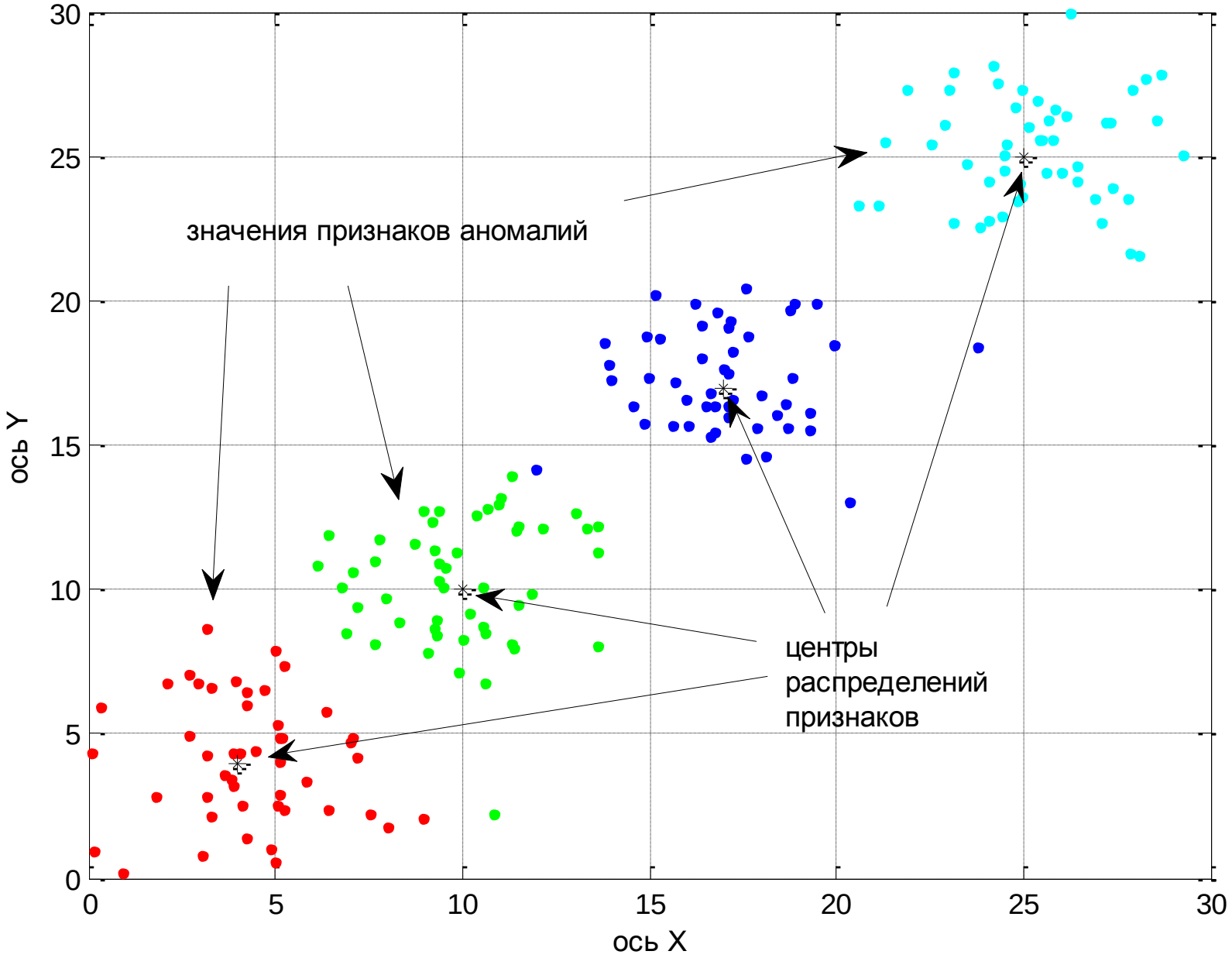


З – затраты атакующего, В – выигрыш атакующего,
П – ожидаемые потери от реализации угроз

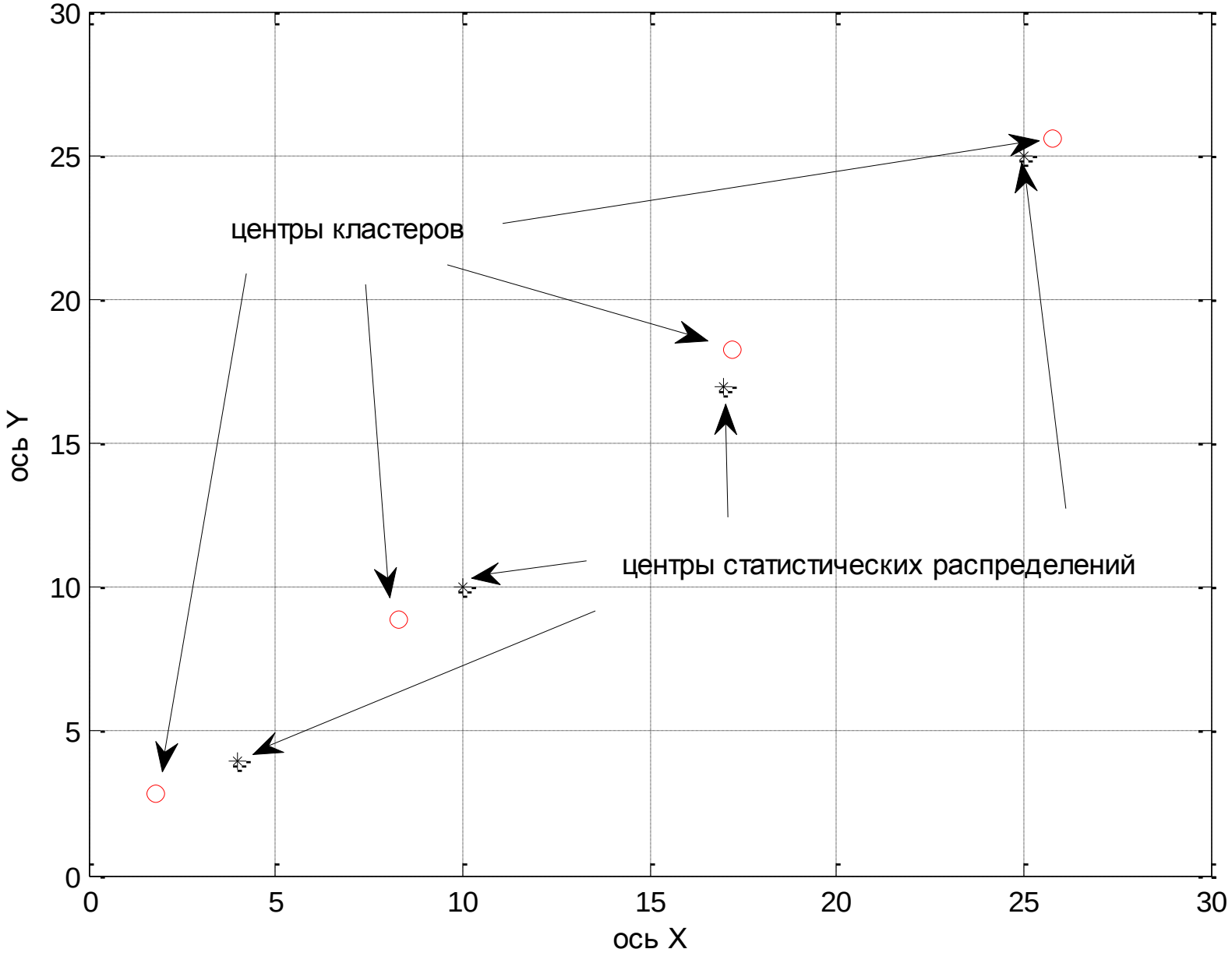
Обобщённая структура процедур кластеризации, классификации и ранжирования



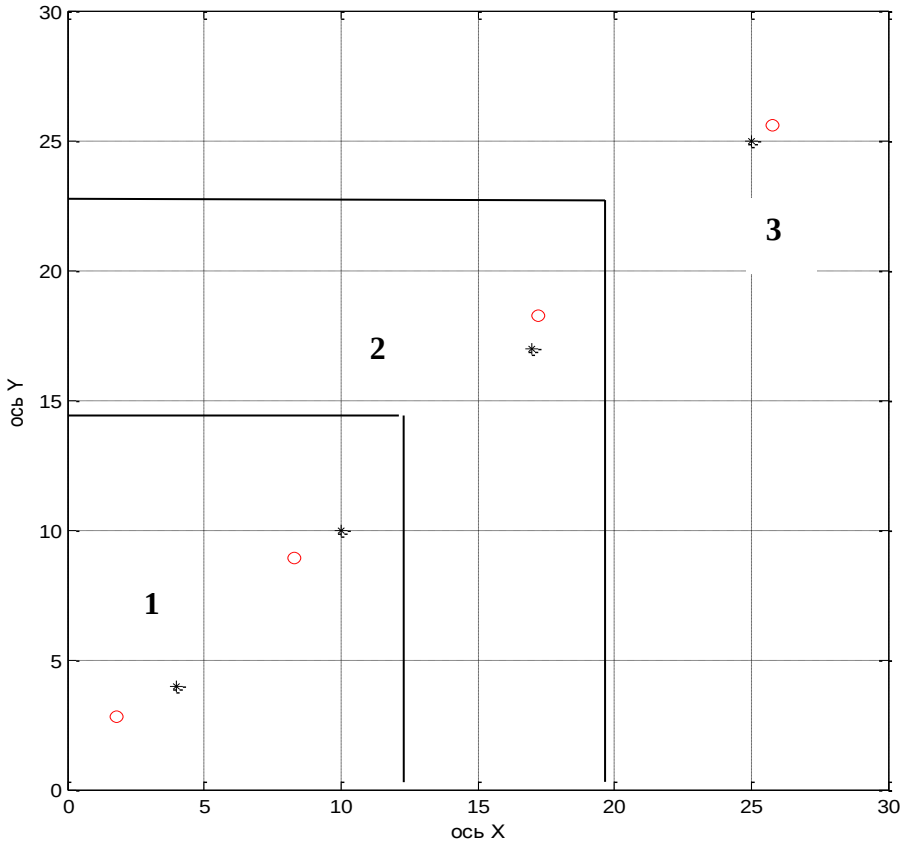
Распределение признаков, центры кластеров

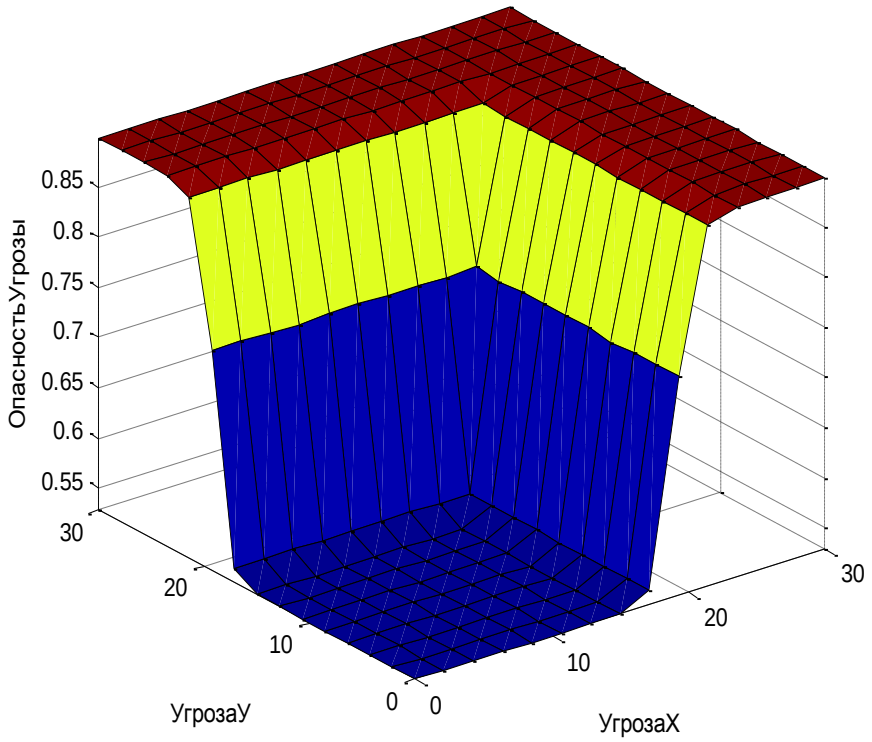


Результаты кластеризации

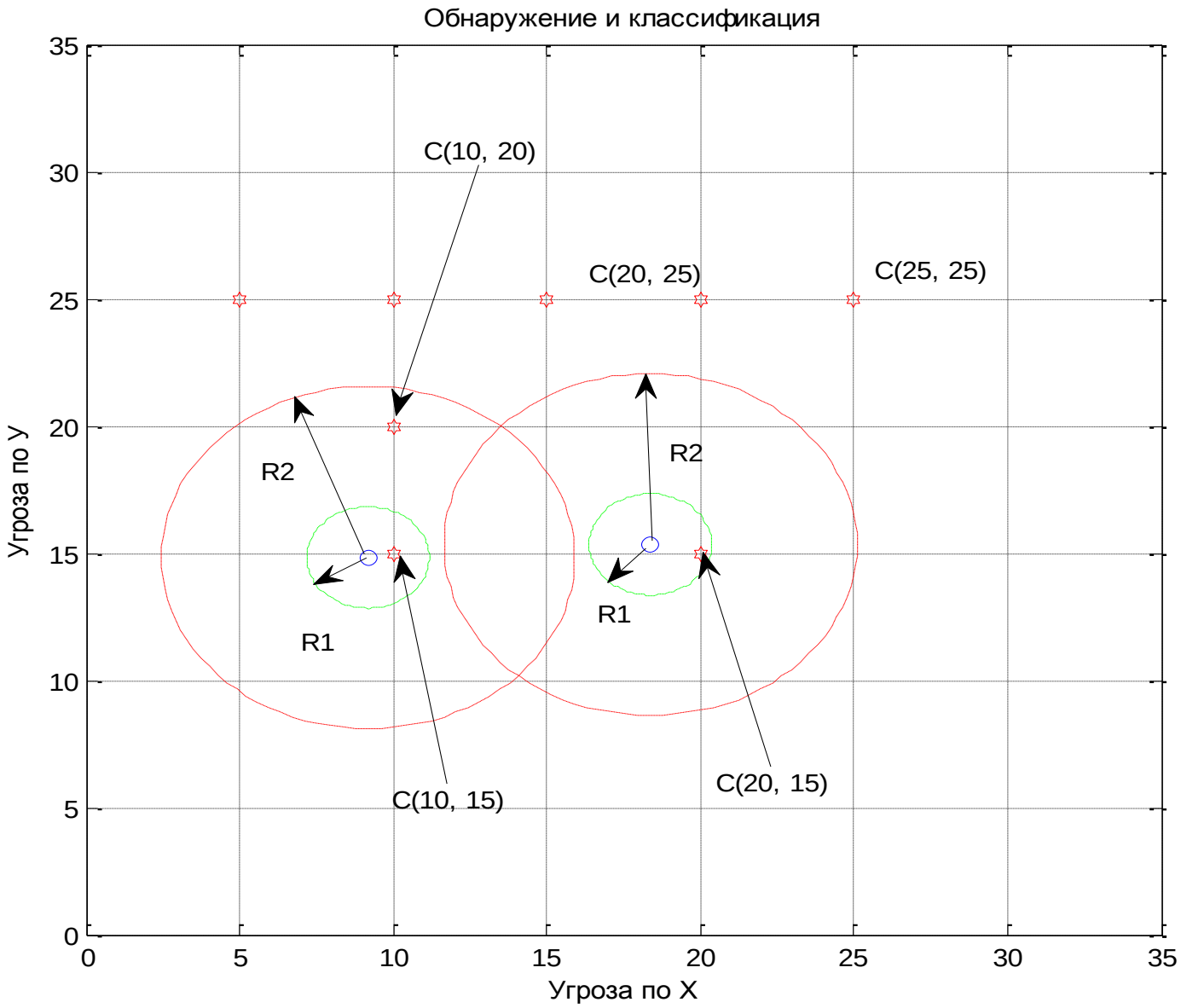


Возможное разбиение пространства признаков и кластеров для оценки степени риска ИБ МСС

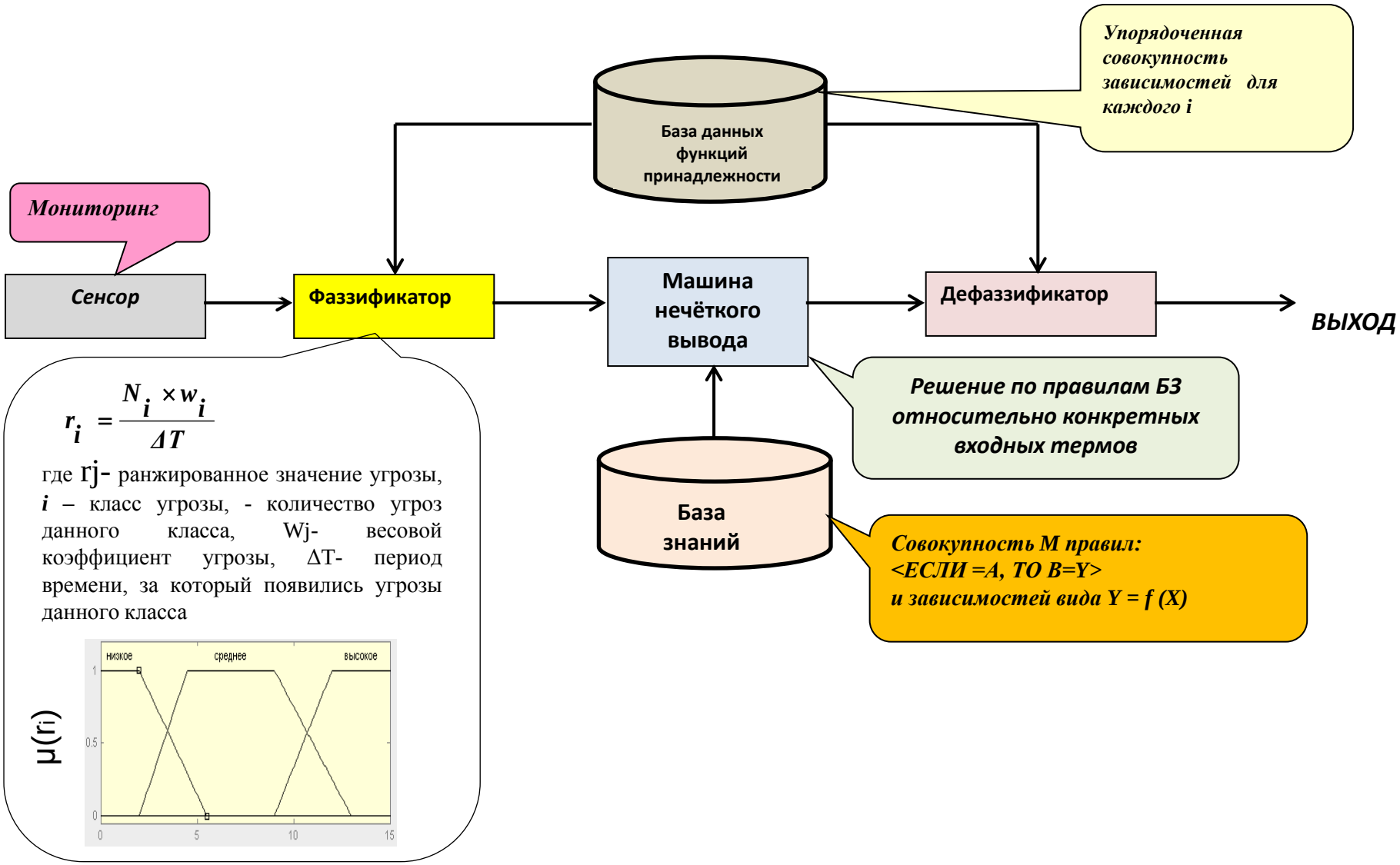




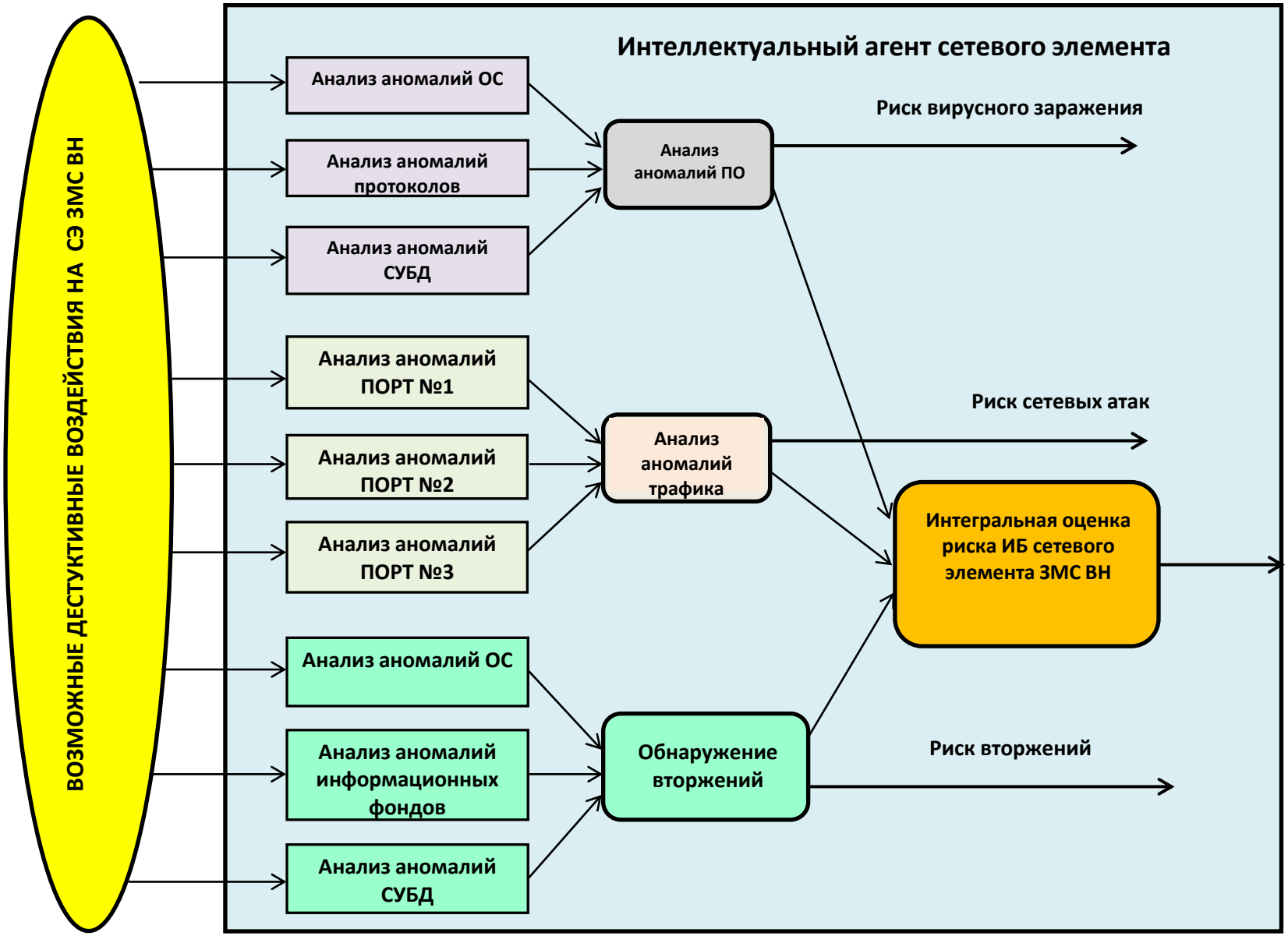
Классификация угроз ИБ СЭ ЗМС СН



ФУНКЦИОНАЛЬНАЯ СХЕМА ИНТЕЛЛЕКТУАЛЬНОГО АГЕНТА В ЧАСТИ ПРИНЯТИЯ РЕШЕНИЙ ПО ОЦЕНКЕ РИСКА ИБ



Структура ИА СЭ МСС



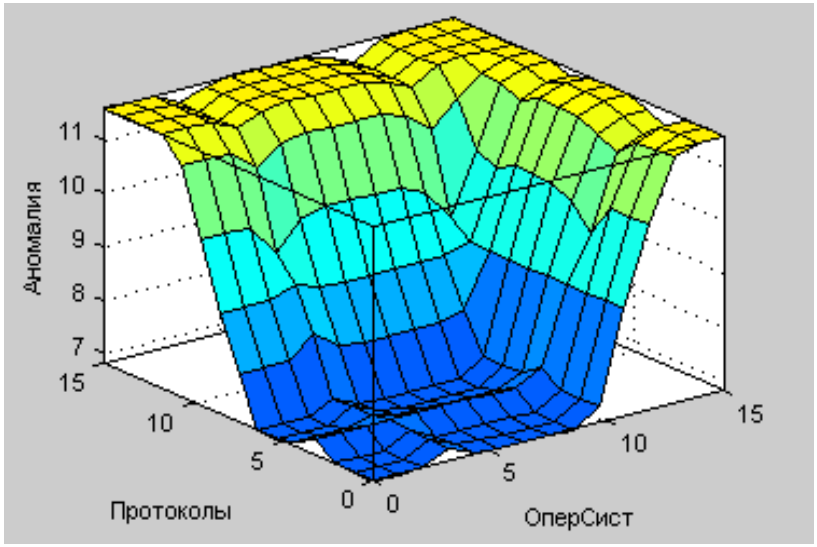
Результаты моделирования интеллектуальной системы оценивания рисков ИБ МСС

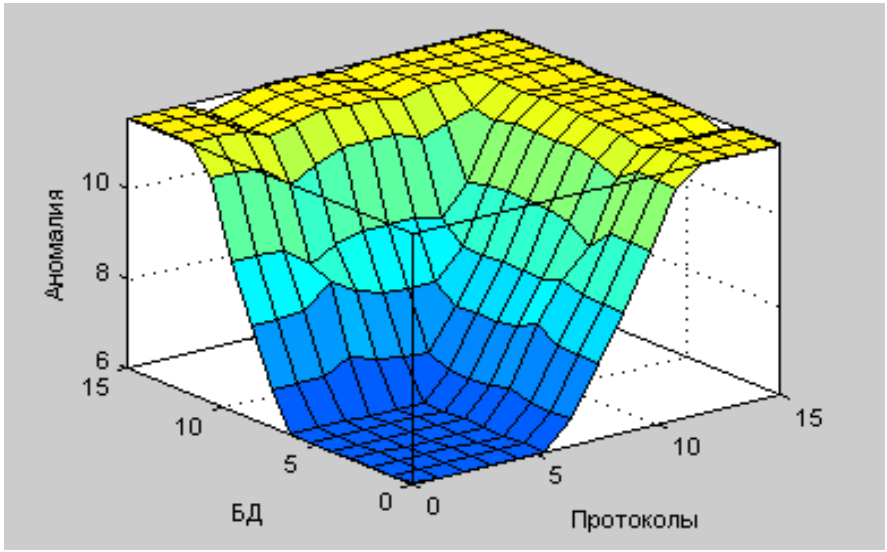
Оцениваются следующие риски ИБ:

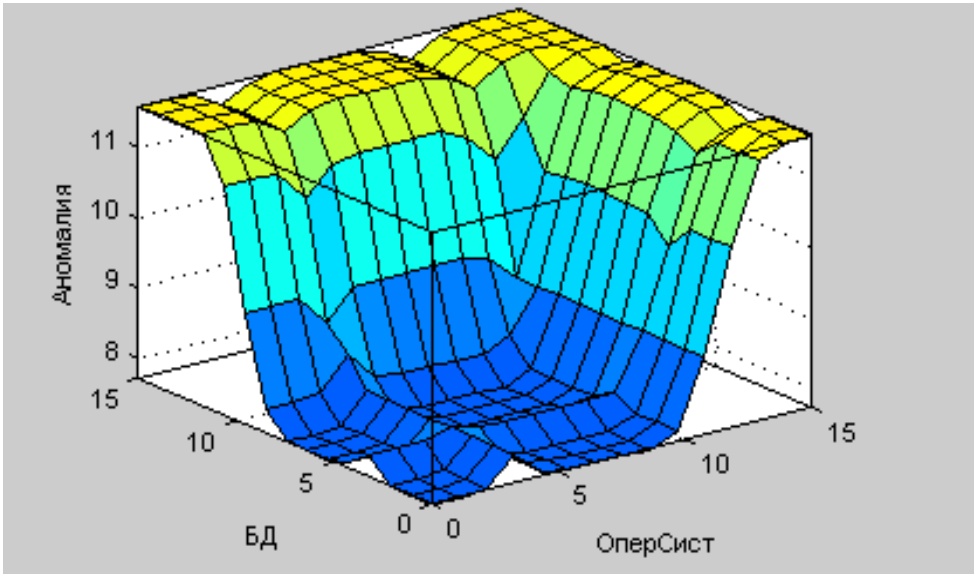
1. Аномалии **общесистемного и специального программного** обеспечения (ОПО и СПО) сетевого элемента в части:
   - операционной системы;
   - протоколов системного взаимодействия;
   - баз данных.
2. Анализ **аномалий входящего и исходящего сетевого трафика** в части:
   - трафика порта № 1;
   - трафика порта № 2;
   - трафика порта № 3.
3. Обнаружений **вторжений** в части:
   - операционной системы;
   - информационных фондов СЭ;
   - баз данных СЭ.

Кроме этого, производится **интегральная оценка рисков** ИБ СЭ МСС в части:
- **аномалий функционирования** ОПО и СПО;
- **входящего и исходящего трафика**;
- обнаружения **вторжений**.

Поверхности ФП «вход-выход» модуля анализа аномалий ПО



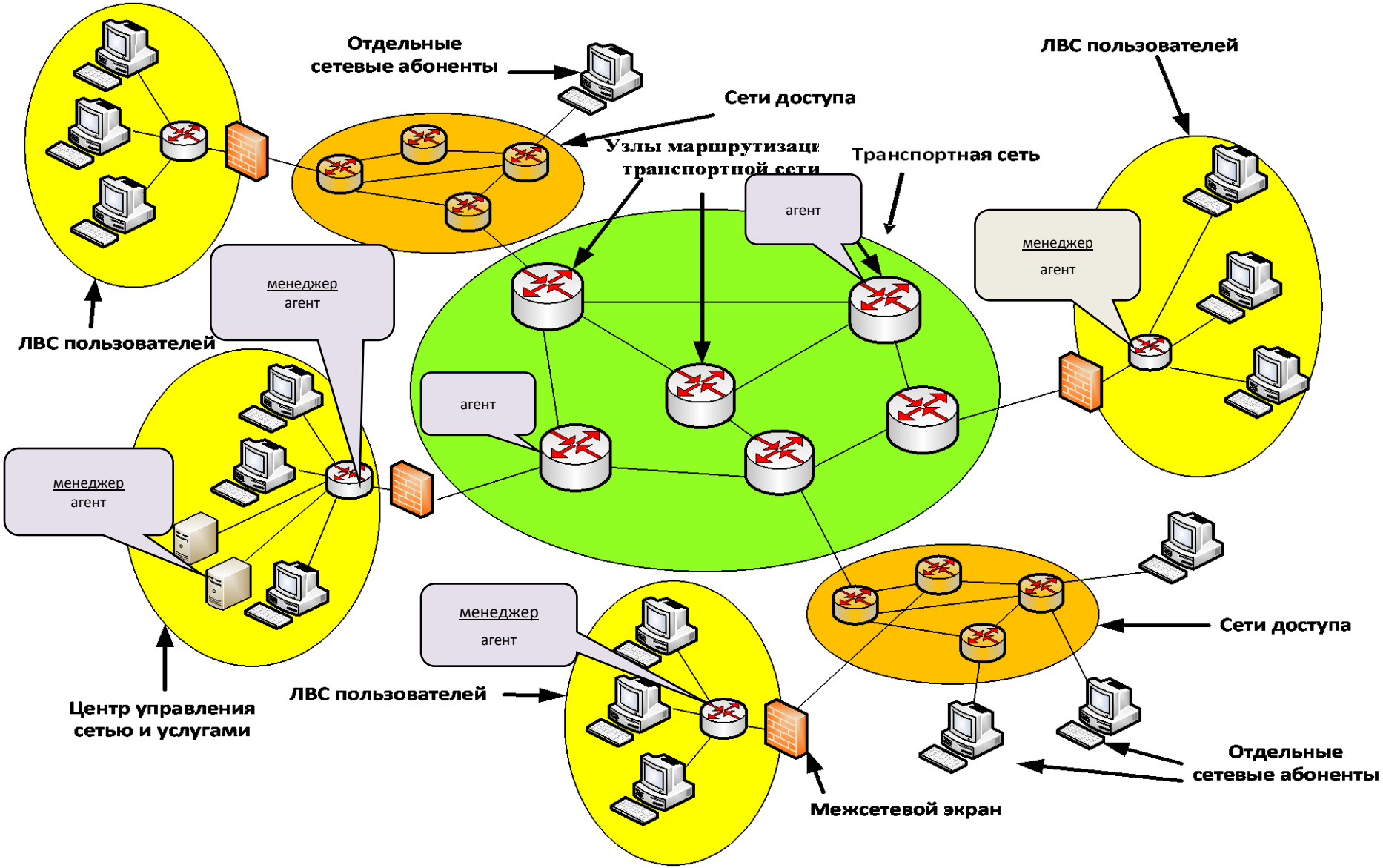




Результаты численного моделирования оценки риска ИБ сетевого элемента методом Мамдани

№/№	Обнаружение аномалий				Оценка риска аномалий трафика				Обнаружение вторжения				Интегральная оценка риска ИБ	
	ОС	Драйвер	Протокол	Выход	Порт 1 [0-50]	Порт 2 [0-50]	Порт 3 [0-50]	Выход [0-50]	ОС [0-12]	Драйвер [0-10]	Протокол [0-10]	Выход [0-12]		
1	0	0	0	1.82	0	0	0	7	0	0	0	1.24	1.3	низкий
2	1	1	1	1.82	1	1	1	7	10	10	10	9.5	10.103	высокий
3	5	5	5	6	5	5	5	7	12	0	0	9.5	10.103	высокий
4	10	10	10	9.9	10	10	10	16	0	10	0	9.5	9.9997	высокий
5	0	0	10	9.84	10	0	10	14.2	0	0	10	9.5	9.984	высокий
6	15	15	15	11.59	50	50	50	42.35	12	10	10	9.5	10.103	высокий
7	0	10	0	10.3	50	0	0	42.35	12	10	0	9.5	10.103	высокий
8	0	0	15	11.59	0	50	0	42.35	0	5	5	5	10.103	высокий
9	10	0	0	7.72	0	0	50	42.35	0	5	0	5	10.04	высокий
10	0	15	0	11.59	25	25	25	26.87	6	0	0	8.01	10.09	высокий
11	15	0	0	11.59	30	30	30	30.2	6	5	5	8.01	10.04	высокий
12	15	15	0	11.59	45	45	45	42.35	2	2	2	3.44	9.998	высокий
13	0	5	0	6	10	20	40	42	3	3	3	5	10.1	высокий
14	6	0	0	6	30	50	0	42.35	5	4	4	6.73	10.07	высокий
15	6	6	6	6	15	15	15	23.5	4	7	7	7.3	6.11	средний
16	0	6	0	6	20	20	20	23.5	10	8	3	9.5	10.103	высокий
17	6	6	0	6	40	40	40	41.4	8	8	8	9.5	10.103	высокий
18	0	6	6	6	0	45	0	41.4	9	9	9	9.5	10.103	высокий
19	7.5	7.5	7.5	7.7	45	15	45	41.4	9	0	9	9.5	10.036	высокий
20	12	12	12	11.59	20	20	50	41.4	9	6	0	9.5	10.103	высокий
21	8	7.5	7.5	7.7	50	10	30	41.4	12	0	5	9.5	10.036	высокий
22	7.5	8	7.5	8.1	5	45	0	41.4	6	10	5	9.5	10.09	высокий
23	7.5	7.5	8	7.7	10	30	50	41.32	6	5	10	9.5	10.036	высокий

Пример размещения ИА на СЭ



Выводы

- Предложенные алгоритмы **устойчивы к вариациям** входных переменных, достаточно просто реализуются в виде программных средств. Значения входных и выходные лингвистических переменных могут уточняться с помощью применения метода α- сечений.
- Применение технологии интеллектуальных агентов позволяет снизить величину технологического трафика, **повысить оперативность принимаемых решений** по сравнению со статистическими методами для рассмотренных задач приблизительно на 25-30%.
- Предложенный подход позволяет **поддерживать** основные сетевые целевые функции в части оценки и управления рисками ИБ МСС **в области Парето-оптимальных значений**, что в условиях динамично изменяющихся внешних условий и воздействий на МСС возможных деструктивных факторов, является достаточным условием успешного ее функционирования.

Сергей Александрович Агеев, к.т.н., доцент
м.т.: (+7) 952-247-26-61
E-mail: serg123_61@mail.ru

Игорь Борисович Саенко, д.т.н., профессор
E-mail: ibsaen@mail.ru

СПАСИБО ЗА ВНИМАНИЕ!