2.12. Анализ безопасности автоматизированной заправочной станции

2.12.1. Описание задачи

Требуется выполнить вероятностный анализ безопасности объекта автоматизированной заправки емкости нефтепродуктами. Укрупненная схема данного объекта изображена на рис.2.12.1 [27].

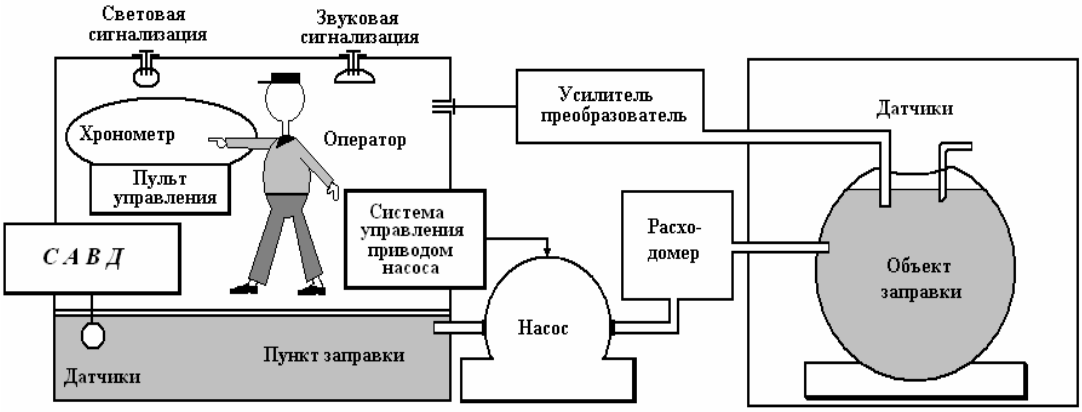


Рис.2.12.1. Объект автоматизированной заправки емкости нефтепродуктами

На основе детального анализа системы, изображенной на рис.2.12.1 (назначения и организации работы элементов автоматизированной заправки, подсистемы автоматической противоаварийной защиты, средств индикации, управления и действий оператора по предотвращению аварии), разработана функциональная блок-схема штатной (безопасной, безаварийной) работы объекта автоматизированной заправки нефтепродуктами, приведенная на рис.2.12.2.

В этой функциональной блок-схеме прямоугольниками 1, 2, 4-6, 11-13 обозначены события безотказной работы технических средств подсистем противоаварийной защиты и управления насосом. Кружками 7-10 на блок-схеме обозначены события, характеризующие штатные (безошибочные) действия оператора.

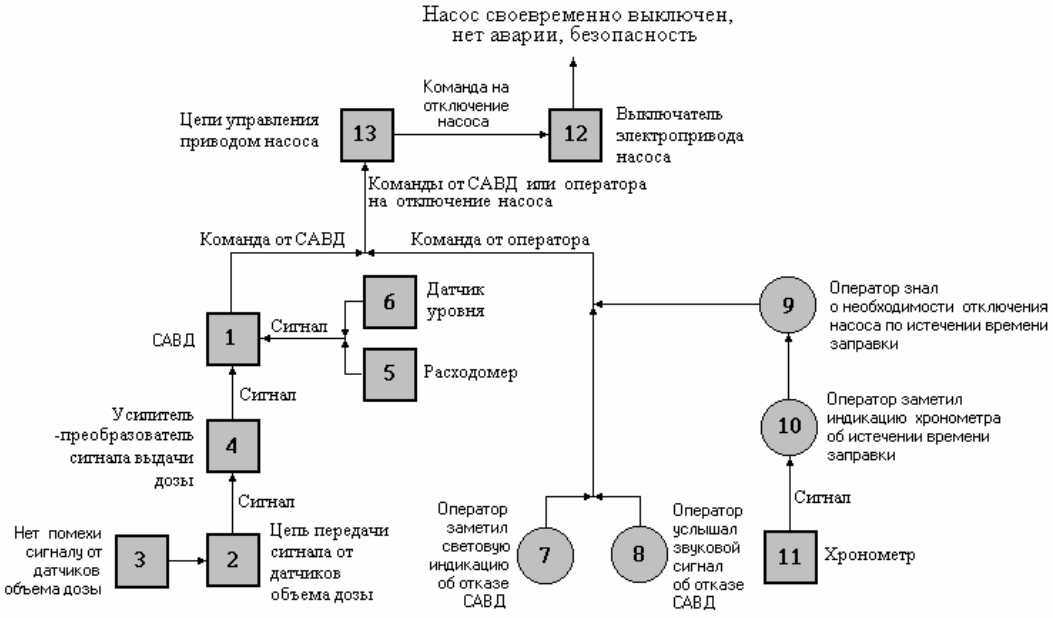


Рис.2.12.2. Функциональная блок-схема безопасности заправочной операции

Краткие описания и заданные вероятности указанных элементарных (исходных) событий приведены в таблице 2.12.1.

Таблица 2.12.1.

Исходные события модели безопасности заправочной операции

№ i	Описание события	Вероятность события p_i
1	Система автоматической выдачи дозы (САВД) оказалась включенной	0,9995
2	Не произошел обрыв цепей передачи сигнала от датчиков объема дозы	0,99999
3	Не произошло ослабления сигнала выдачи дозы помехами	0,9999
4	Не отказал усилитель-преобразователь сигнала выдачи дозы	0,9998
5	Не отказал расходомер	0,9997
6	Не отказал датчик уровня	0,9998
7	Оператор заметил световую индикацию о неисправности САВД	0,995
8	Оператор услышал звуковую сигнализацию об отказе САВД	0,999
9	Оператор знал о необходимости отключения насоса по истечении заданного времени	0,999
10	Оператор заметил индикацию хронометра об истечении заданного времени заправки	0,996
11	Хронометр не отказал	0,99999
12	Не отказал автоматический выключатель электропривода насоса	0,99999
13	Не произошел обрыв в цепи управления приводом насоса	0,99999

2.12.2. Результаты решения на ПК «RELEX»

Тестовый расчет проведен в модулях Relex Деревьев Отказов (Relex Fault Tree) и Блок-Схем Надежности.

Дерево отказов представлено на рис. 2.12.3.

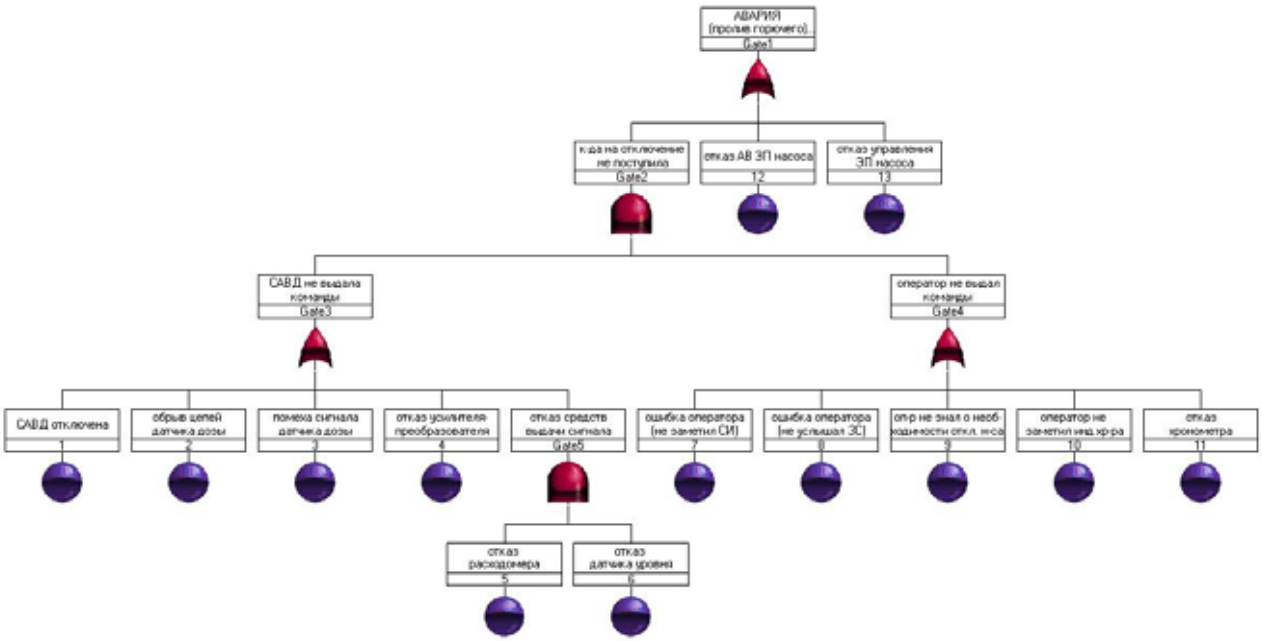


Рис. 2.12.3 Дерево отказов для аварии на заправочной станции

Список базисных событий дерева и значений соответствующих вероятностей приведен в таблице 2.12.2.

Таблица 2.12.2.

Исходные события дерева отказов заправочной станции

№ i	Описание события	Вероятность события p_i
1	Система автоматической выдачи дозы (САВД) оказалась отключенной (ошибка контроля исходного положения	0,0005
2	Обрыв цепей передачи сигнала от датчиков объема дозы	0,00001
3	Ослабления сигнала выдачи дозы помехами (нерасчетное внешнее воздействие)	0,0001
4	Отказ усилителя-преобразователя сигнала выдачи дозы	0,0002
5	Отказ расходомера	0,0003
6	Отказ датчика уровня	0,0002
7	Оператор не заметил световой индикации о неисправности САВД (ошибка оператора)	0,005
8	Оператор не услышал звуковой сигнализации об отказе САВД (ошибка оператора)	0,001
9	Оператор не знал о необходимости отключения насоса по истечении заданного времени	0,001
10	Оператор не заметил индикации хронометра об истечении установленного времени заправки	0,004
11	Отказ хронометра	0,00001
12	Отказ автоматического выключателя электропривода насоса	0,00001
13	Обрыв цепей управления приводом насоса	0,00001

В результате расчета на дереве отказов, построенном в модуле Relex Fault Tree, получено значение вероятности возникновения аварии заправочной станции

P{аварии} = 0.00002888.

Пример 12 был решен в постановке задачи, данной в методических материалах Госгортехнадзора. Однако, по нашему мнению, такая постановка является упрощенной и не содержит специфичных, именно для анализа безопасности, особенностей. Кроме того, хотелось бы отметить, что для данной постановки задачи не совсем обоснованным является привлечение аппарата деревьев отказов, так как решение может быть получено гораздо более простыми способами. В частности, можно использовать блок-схемы надежности последовательно-параллельных систем. Блок-схема для решения задачи анализа безопасности заправочной станции, набранная в модуле Relex RBD, представлена рис. 2.12.8.

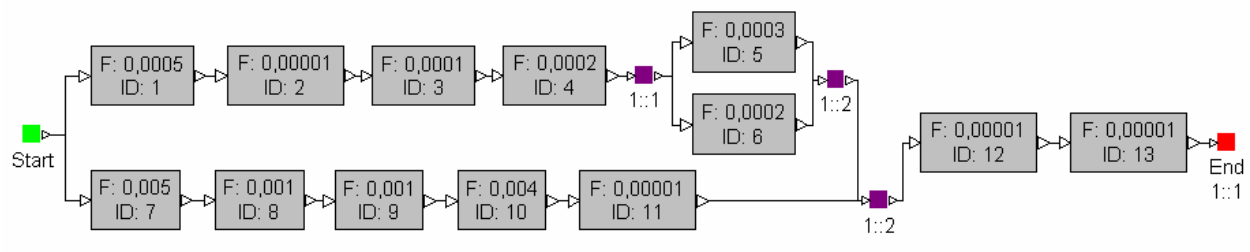


Рис. 2.11.4. Блок-схема безопасности автоматизированной заправочной станции

В результате расчета получено значение вероятности возникновения аварии

P{аварии} = 0.0000288849.

Другим, еще более простым способом, является решение по формуле:

$$P\{\text{отсутствия аварии}\}=(1-(1-P_1*P_2*P_3*P_4*(P_5+Q_5*P_6))(1-P_7*P_8*P_9*P_{10}*P_{11}))*P_{12}*P_{13},$$

где Pi взяты из таблицы 2.12.1.

Формульное выражение позволяет получить еще более точный результат для вероятности отсутствия аварии на заправочной станции, равный

P {отсутствия аварии} = 0.999971115111788

2.12.3. Результаты решения на ПК «АСМ»

Указанных в п. 2.12.1 данных достаточно, чтобы приступить к разработке СФЦ, необходимой для автоматизированного вероятностного анализа безопасности рассматриваемой заправочной операции.

СФЦ могут быть двух видов. На основе прямой логики рассуждений может быть построена СФЦ, представляющая условия безопасного выполнения заправочной операции. На основе обратной логики рассуждений может быть построена СФЦ противоположной структурной модели возникновения аварии в процессе выполнения заправочной операции. Оба указанных вида структурных моделей эквивалентны, т.е. каждая из них дает одинаковые результаты ВАБ. Разница заключается только в простоте, удобстве и точности построения СФЦ того или иного вида. Право выбора вида разрабатываемой СФЦ в технологии АСМ предоставляется пользователю. В данном тестовом примере рассмотрим оба варианта.

Пример 1. Решение задачи ВАБ заправочной станции на основе СФЦ безопасности

В данном случае для построения СФЦ применяется прямая логика рассуждений. На основе знаний объекта исследования (см. рис.2.12.1), функциональной блок-схемы безопасности заправочной операции (см. рис.2.12.2) и состава ее элементов (см. таблицу 2.12.1) определяются логические условия штатного (правильного, безаварийного) функционирования исследуемой системы. Безопасностью (отсутствием события аварии) в данном случае является не пролив горючего, т.е. не переполнение емкости из-за излишней продолжительности работы насоса вследствие его не отключения вовремя (сразу после окончания заполнения емкости). В рассматриваемой задаче таких основных условий может быть выделено всего три.

1. Команда на выключение насоса может быть выдана автоматически от САВД на основе обработки сигналов от датчиков;
2. Команда на выключение насоса может быть выдана вручную оператором на основе анализа показателей индикаторов процесса заправки;
3. После автоматической или ручной выдачи указанной команды должна безотказно выполнить свои функции подсистема выключения насоса.

На рис. 2.12.5. изображены фрагменты СФЦ, представляющие реализованную в данной системе логику совместной работы элементов и действий оператора, обеспечивающих реализацию указанных трех условий безопасного выполнения заправочной операции.

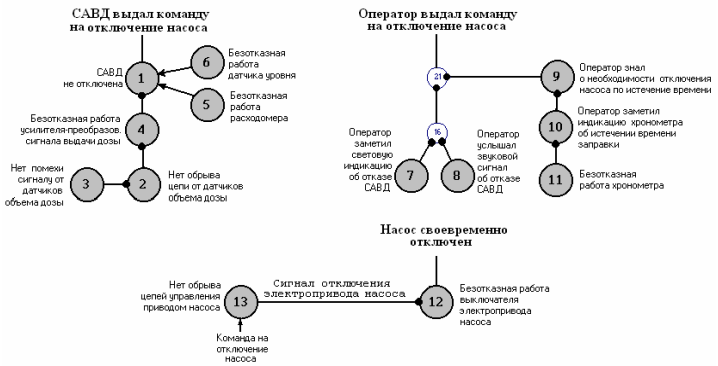


Рис.2.12.5. Фрагменты СФЦ реализации основных условий безопасности заправочной операции

Объединяя разработанные фрагменты, получаем СФЦ безопасности заправочной операции. Она изображена на рис.2.12.6.а.

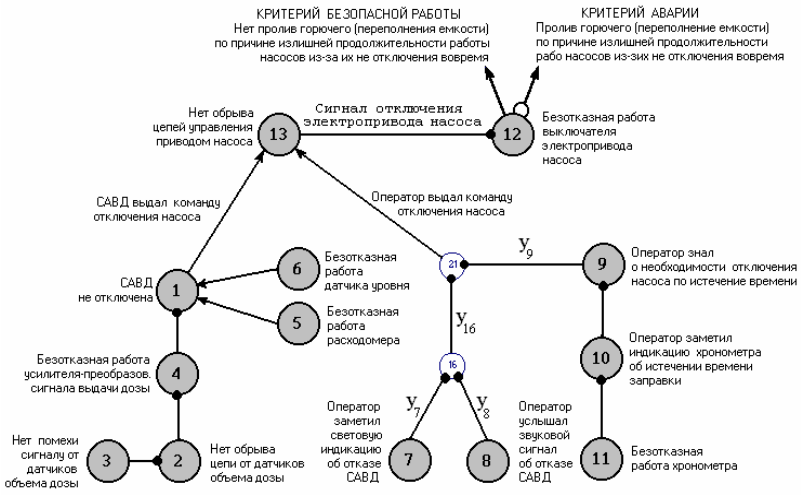


Рис.2.12.6.а. СФЦ безопасности заправочной операции

Как видим данная СФЦ является прямым подобием исходной блок-схемы исследуемоемой системы (см.рис.2.12.2), поэтому ее построение не вызывает затруднений.

Выполняя на основе данной СФЦ и критерия безопасности $Y_{безопасности} = y_{12}$ автоматизированное моделирование и расчет с помощью ПК АСМ получаем:

$$Y_{безопасности} = y_{12} = x_1 \cdot x_2 \cdot x_3 \cdot x_4 \cdot x_5 \cdot x_{12} \cdot x_{13} \vee x_1 \cdot x_2 \cdot x_3 \cdot x_4 \cdot x_6 \cdot x_{12} \cdot x_{13} \vee \vee x_7 \cdot x_8 \cdot x_9 \cdot x_{10} \cdot x_{11} \cdot x_{12} \cdot x_{13}$$

$$P_{безопасности} = p_1 p_2 p_3 p_4 p_5 q_6 p_{12} p_{13} + p_7 p_8 p_9 p_{10} p_{11} p_{12} p_{13} + p_1 p_2 p_3 p_4 p_6 p_{12} p_{13} - p_1 p_2 p_3 p_4 p_6 p_7 p_8 p_9 p_{10} p_{11} p_{12} p_{13} - p_1 p_2 p_3 p_4 p_5 q_6 p_7 p_8 p_9 p_{10} p_{11} p_{12} p_{13} = 0.99997111\,5112$$

Логическая модель точно совпала с КПУФ данной системы, приведенными в РД 03-418-01, а расчет вероятности безопасности практически совпал с результатом решения этой задачи, полученным с помощью модуля Relex RBD.

На основе той же СФЦ, изображенной на рис.2.12.6.а, задавая критерий аварии $Y_{аварии} = \overline{y}_{12}$ получаем с помощью ПК АСМ точные противоположные логические и вероятностные модели данной системы.

$$Y_{аварии} = y''_{12} = \overline{x}_1 \cdot \overline{x}_7 \vee \overline{x}_2 \cdot \overline{x}_7 \vee \overline{x}_3 \cdot \overline{x}_7 \vee \overline{x}_4 \cdot \overline{x}_7 \vee \overline{x}_5 \cdot \overline{x}_6 \cdot \overline{x}_7 \vee \overline{x}_1 \cdot \overline{x}_8 \vee \overline{x}_2 \cdot \overline{x}_8 \vee \overline{x}_3 \cdot \overline{x}_8 \vee \overline{x}_4 \cdot \overline{x}_8 \vee \overline{x}_5 \cdot \overline{x}_6 \cdot \overline{x}_8 \vee \overline{x}_1 \cdot \overline{x}_9 \vee \overline{x}_2 \cdot \overline{x}_9 \vee \overline{x}_3 \cdot \overline{x}_9 \vee \overline{x}_4 \cdot \overline{x}_9 \vee \overline{x}_5 \cdot \overline{x}_6 \cdot \overline{x}_9 \vee \overline{x}_1 \cdot \overline{x}_{10} \vee \overline{x}_2 \cdot \overline{x}_{10} \vee \overline{x}_3 \cdot \overline{x}_{10} \vee \overline{x}_4 \cdot \overline{x}_{10} \vee \overline{x}_5 \cdot \overline{x}_6 \cdot \overline{x}_{10} \vee \overline{x}_1 \cdot \overline{x}_{11} \vee \overline{x}_2 \cdot \overline{x}_{11} \vee \overline{x}_3 \cdot \overline{x}_{11} \vee \overline{x}_4 \cdot \overline{x}_{11} \vee \overline{x}_5 \cdot \overline{x}_6 \cdot \overline{x}_{11} \vee \overline{x}_{12} \vee \overline{x}_{13}$$

$$P_{аварии} = q3\ q11\ p12\ p13 + q2\ p3\ q11\ p12\ p13 + p2\ p3\ q4\ q11\ p12\ p13 + p1\ p2\ p3\ p4\ q5\ q6\ q11\ p12\ p13 + q1\ p2\ p3\ p4\ q11\ p12\ p13 + q3\ q10\ p11\ p12\ p13 + q2\ p3\ q10\ p11\ p12\ p13 + p2\ p3\ q4\ q10\ p11\ p12\ p13 + p1\ p2\ p3\ p4\ q5\ q6\ q10\ p11\ p12\ p13 + q1\ p2\ p3\ p4\ q10\ p11\ p12\ p13 + q3\ q9\ p10\ p11\ p12\ p13 + q2\ p3\ q9\ p10\ p11\ p12\ p13 + p2\ p3\ q4\ q9\ p10\ p11\ p12\ p13 + p1\ p2\ p3\ p4\ q5\ q6\ q9\ p10\ p11\ p12\ p13 + q1\ p2\ p3\ p4\ q9\ p10\ p11\ p12\ p13 + q3\ q8\ p9\ p10\ p11\ p12\ p13 + q2\ p3\ q8\ p9\ p10\ p11\ p12\ p13 + p2\ p3\ q4\ q8\ p9\ p10\ p11\ p12\ p13 + p1\ p2\ p3\ p4\ q5\ q6\ q8\ p9\ p10\ p11\ p12\ p13 + q1\ p2\ p3\ p4\ q8\ p9\ p10\ p11\ p12\ p13 + q3\ q7\ p8\ p9\ p10\ p11\ p12\ p13 + q2\ p3\ q7\ p8\ p9\ p10\ p11\ p12\ p13 + p2\ p3\ q4\ q7\ p8\ p9\ p10\ p11\ p12\ p13 + p1\ p2\ p3\ p4\ q5\ q6\ q7\ p8\ p9\ p10\ p11\ p12\ p13 + q1\ p2\ p3\ p4\ q7\ p8\ p9\ p10\ p11\ p12\ p13 + q13 + q12\ p13 = \mathbf{0.000028884888}$$

Пример 2. Решение задачи ВАБ на основе СФЦ дерева отказа заправочной станции

Теперь выполним ВАБ рассматриваемой заправочной операции, используя для построения исходной структурной модели не прямую, а обратную логику рассуждений. Именно такой подход применяется в технологиях и программных комплексах, в которых в качестве исходной структурной схемы системы используются деревья отказов.

Для построения СФЦ аварии (дерева отказа) необходимо на основе знаний объекта исследования, его функциональной блок-схемы безопасности и состава элементов определить не условия штатного (безаварийного, безопасного) выполнения заправочной операции (что было выполнено в предыдущем решении), а все возможные условия нарушения этого штатного функционирования, приводящие к возникновению аварии. Теперь для постановки задачи ВАБ надо определить и графически отобразить в СФЦ аварии (дереве отказа) все комбинации отказов элементов, приводящие к проливу горючего, т.е. переполнению емкости из-за излишней продолжительности работы насоса вследствие его не отключения вовремя. Не трудно видеть, что для выделения указанных условий возникновения аварии и последующего их представления с помощью СФЦ, все равно, сначала необходимо определить условия штатного, безаварийного функционирования исследуемой системы, поскольку только на основе этих знаний можно правильно определить условия возникновения аварии.

Проиллюстрируем сказанное. Ранее мы выделили три условия штатного, безаварийного выполнения заправочной операции. На рис.2.12.5 они представлены соответствующими тремя фрагментами СФЦ. Естественно, что в структурной модели аварии необходимо отобразить все возможные варианты нарушения (не выполнения) каждого из указанных штатных условий безаварийной работы системы.

Варианты таких фрагментов СФЦ приведены в правой части рис.2.12.6.б. Для удобства сравнения и контроля их правильности, в левой части рис.2.12.6.б повторены фрагменты ранее разработанных СФЦ реализации условий безопасности заправочной операции.

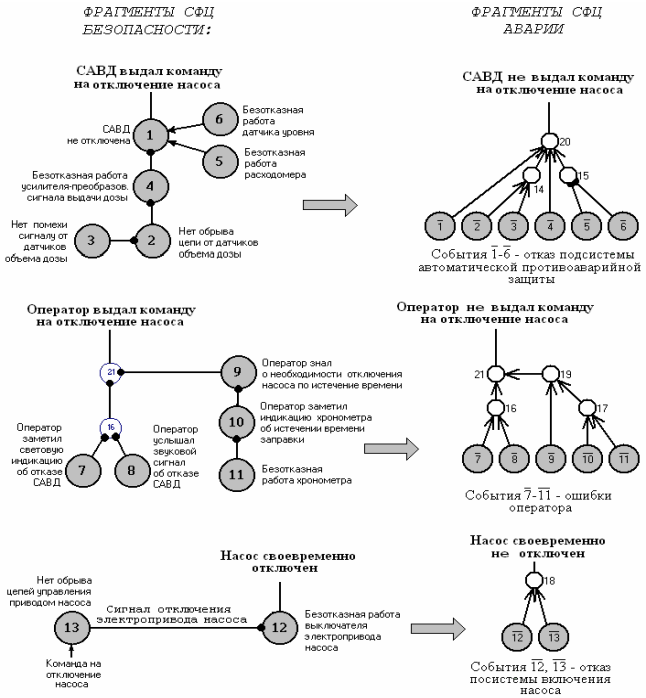


Рис.2.12.6.б. Разработка фрагментов СФЦ нарушения условий безопасного выполнения заправочной операции

Все элементарные события в СФЦ правой части рис.2.12.6.б представлены противоположными исходами (отказами, ошибками), по отношению к событиям, которые использовались ранее, при построении СФЦ безопасности. На рис.2.12.6.б номера противоположных элементарных событий помечены знаками инверсирования.

Объединяя фрагменты правой части рис.2.12.6.б. получаем СФЦ аварии (дерево отказа) рассматриваемой заправочной операции. Она изображена на рис.2.12.7.

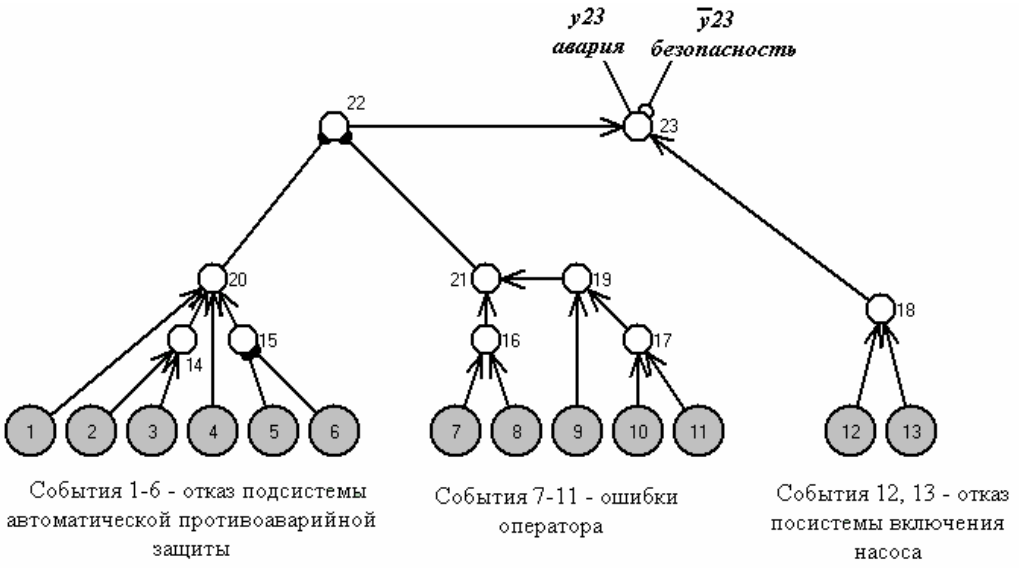


Рис.2.12.7. СФЦ аварии заправочной операции

Все исходные события $i = 1,2,...,13$ в этой СФЦ противоположны событиям модели безопасности, а их вероятности являются дополнениями соответствующих параметров, указанных в таблице 2.12.1. Выполняя моделирование аварии этой системы на ПК АСМ по критерию $Y_{аварии} = y_{23}$, получаем:

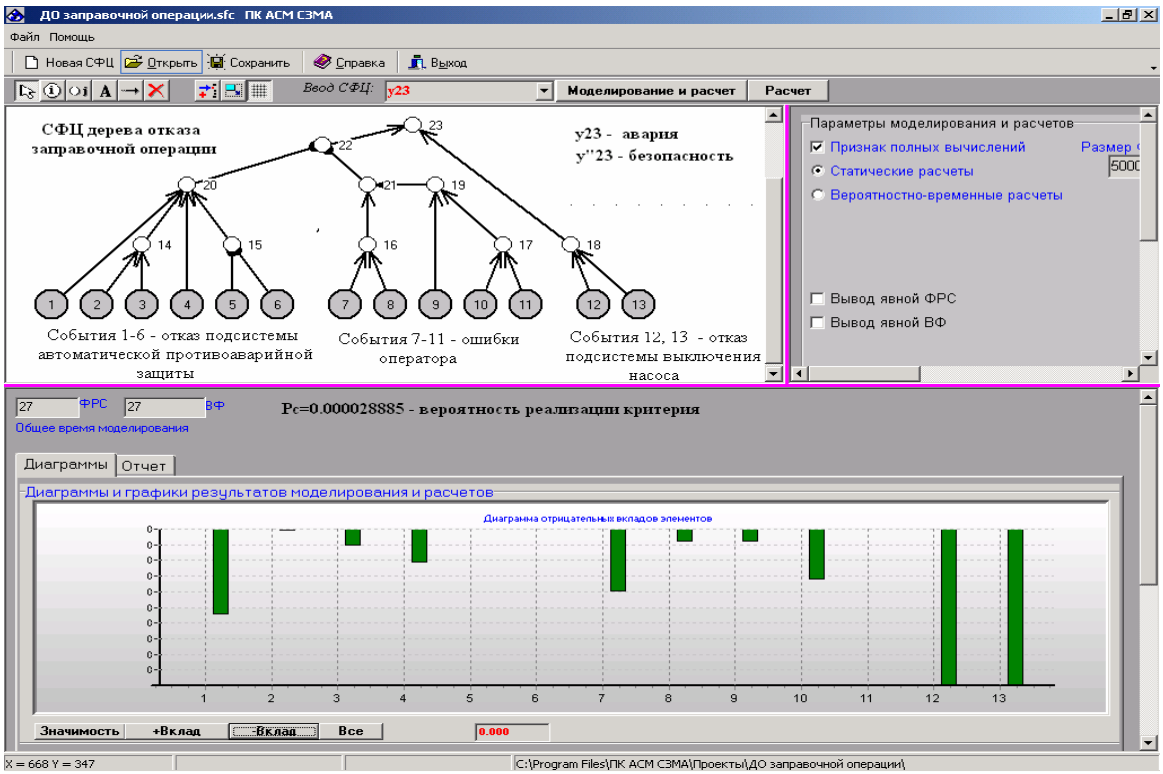


Рис.2.12.8. Моделирование и расчет аварии заправочной операции на ПК АСМ СЗМА

Логическая модель аварии:

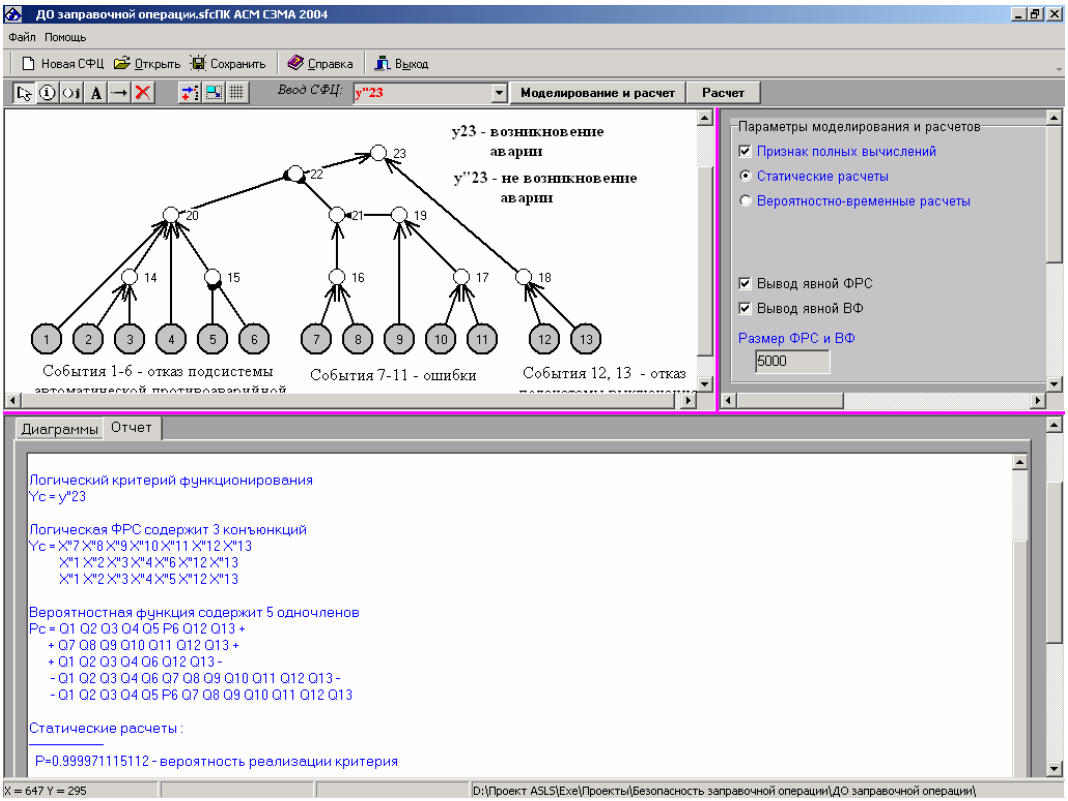
$$Y_{аварии} = y_{23} = x_1 \cdot x_7 \vee x_2 \cdot x_7 \vee x_3 \cdot x_7 \vee x_4 \cdot x_7 \vee x_5 \cdot x_6 \cdot x_7 \vee x_1 \cdot x_8 \vee x_2 \cdot x_8 \vee$$
$$\vee x_3 \cdot x_8 \vee x_4 \cdot x_8 \vee x_5 \cdot x_6 \cdot x_8 \vee x_1 \cdot x_9 \vee x_2 \cdot x_9 \vee x_3 \cdot x_9 \vee x_4 \cdot x_9 \vee$$
$$\vee x_5 \cdot x_6 \cdot x_9 \vee x_1 \cdot x_{10} \vee x_2 \cdot x_{10} \vee x_3 \cdot x_{10} \vee x_4 \cdot x_{10} \vee x_5 \cdot x_6 \cdot x_{10} \vee$$
$$\vee x_1 \cdot x_{11} \vee x_2 \cdot x_{11} \vee x_3 \cdot x_{11} \vee x_4 \cdot x_{11} \vee x_5 \cdot x_6 \cdot x_{11} \vee x_{12} \vee x_{13}$$

Вероятностная модель аварии:

$$P_{аварии} = p1\ p7\ q12\ q13 + q1\ p2\ p7\ q12\ q13 + q1\ q2\ p3\ p7\ q12\ q13 +$$
$$+\ q1\ q2\ q3\ p4\ p7\ q12\ q13 + q1\ q2\ q3\ q4\ p5\ p6\ p7\ q12\ q13 +$$
$$+\ p1\ q7\ p8\ q12\ q13 + q1\ p2\ q7\ p8\ q12\ q13 +$$
$$+\ q1\ q2\ p3\ q7\ p8\ q12\ q13 + q1\ q2\ q3\ p4\ q7\ p8\ q12\ q13 +$$
$$+ q1\ q2\ q3\ q4\ p5\ p6\ q7\ p8\ q12\ q13 + p1\ q7\ q8\ p9\ q12\ q13 +$$
$$+\ q1\ p2\ q7\ q8\ p9\ q12\ q13 + q1\ q2\ p3\ q7\ q8\ p9\ q12\ q13 +$$
$$+\ q1\ q2\ q3\ p4\ q7\ q8\ p9\ q12\ q13 + q1\ q2\ q3\ q4\ p5\ p6\ q7\ q8\ p9\ q12\ q13 +$$
$$+\ p1\ q7\ q8\ q9\ p10\ q12\ q13 + q1\ p2\ q7\ q8\ q9\ p10\ q12\ q13 +$$
$$+\ q1\ q2\ p3\ q7\ q8\ q9\ p10\ q12\ q13 + q1\ q2\ q3\ p4\ q7\ q8\ q9\ p10\ q12\ q13 +$$
$$+ q1\ q2\ q3\ q4\ p5\ p6\ q7\ q8\ q9\ p10\ q12\ q13 + p1\ q7\ q8\ q9\ q10\ p11\ q12\ q13 +$$
$$+ q1\ p2\ q7\ q8\ q9\ q10\ p11\ q12\ q13 + q1\ q2\ p3\ q7\ q8\ q9\ q10\ p11\ q12\ q13 +$$
$$+ q1\ q2\ q3\ p4\ q7\ q8\ q9\ q10\ p11\ q12\ q13 +$$
$$+\ q1\ q2\ q3\ q4\ p5\ p6\ q7\ q8\ q9\ q10\ p11\ q12\ q13 + p12 + q12\ p13 = 0.000028884888$$

Логическая модель точно совпала с МСО данной системы, приведенными в РД 03-418-01, а расчет вероятности безопасности практически совпал с результатом решения этой задачи, полученным с помощью модуля Relex Fault Tree.

На основе той же СФЦ, изображенной на рис.2.12.7, задавая критерий $Y_{,безопасности} = \overline{y}_{23}$ получаем с помощью ПК АСМ точные противоположные логические и вероятностные модели безопасности данной системы.



2.12.4. Результаты решения на ПК «RISK SPECTRUM»

Дерево отказов АЗС, построенное в редакторе деревьев отказов ПК «Risk Spectrum», представлено на рисунке 2.12.9. Оно совершенно аналогично (с учетом другой системы используемых графических элементов) СФЦ, представленной на 2.12.7 и 2.12.8.

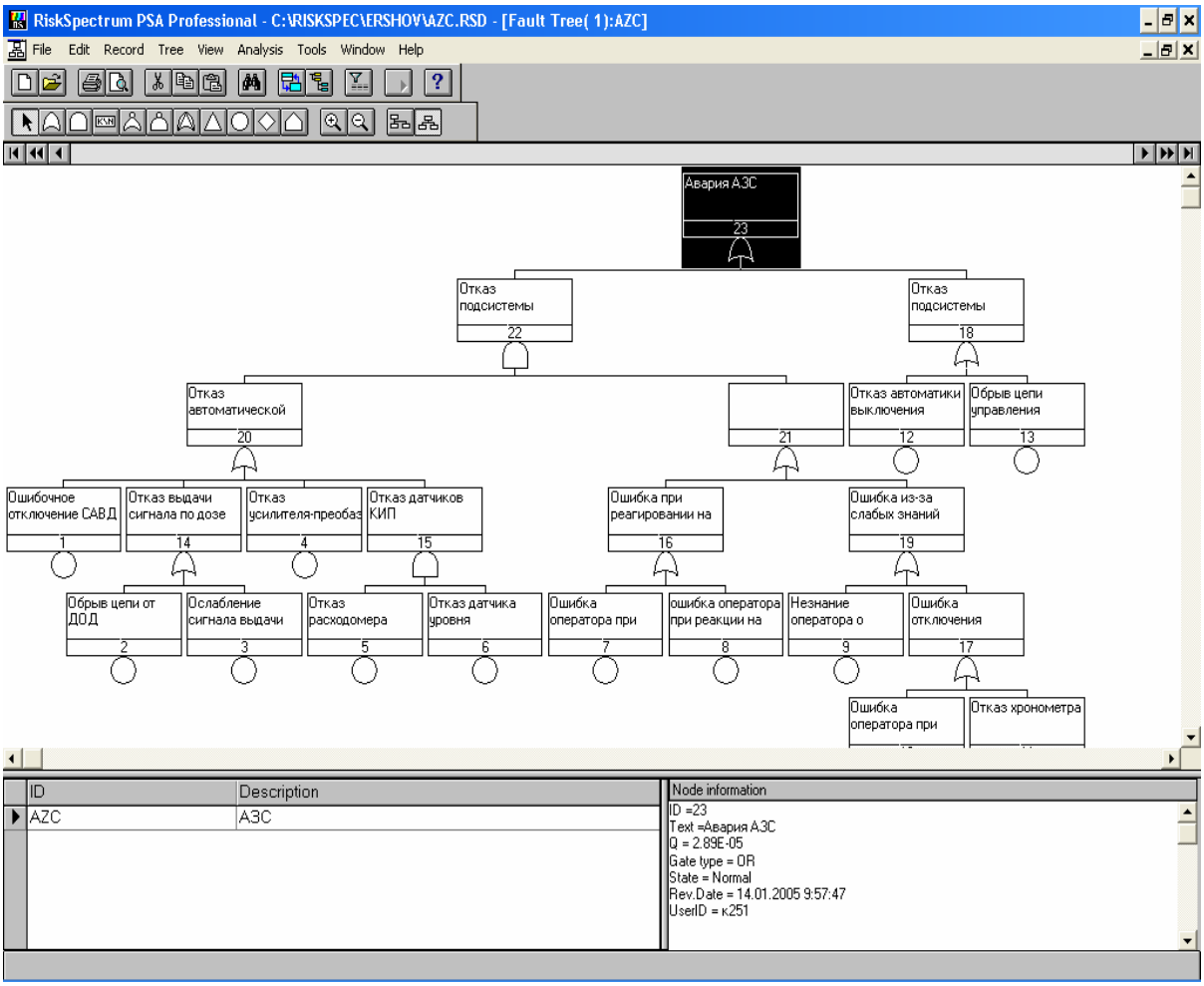


Рис. 2.12.9. Дерево отказов АЗС

Результаты расчетов представлены на рис. 2.12.10, а перечень минимальных сечений – на рис. 2.12.11. Расчеты проведены при использовании третьего уровня аппроксимации.

Как следует из данных рисунков, результаты моделирования и расчета полностью совпали с результатами расчетов по другим ПК.

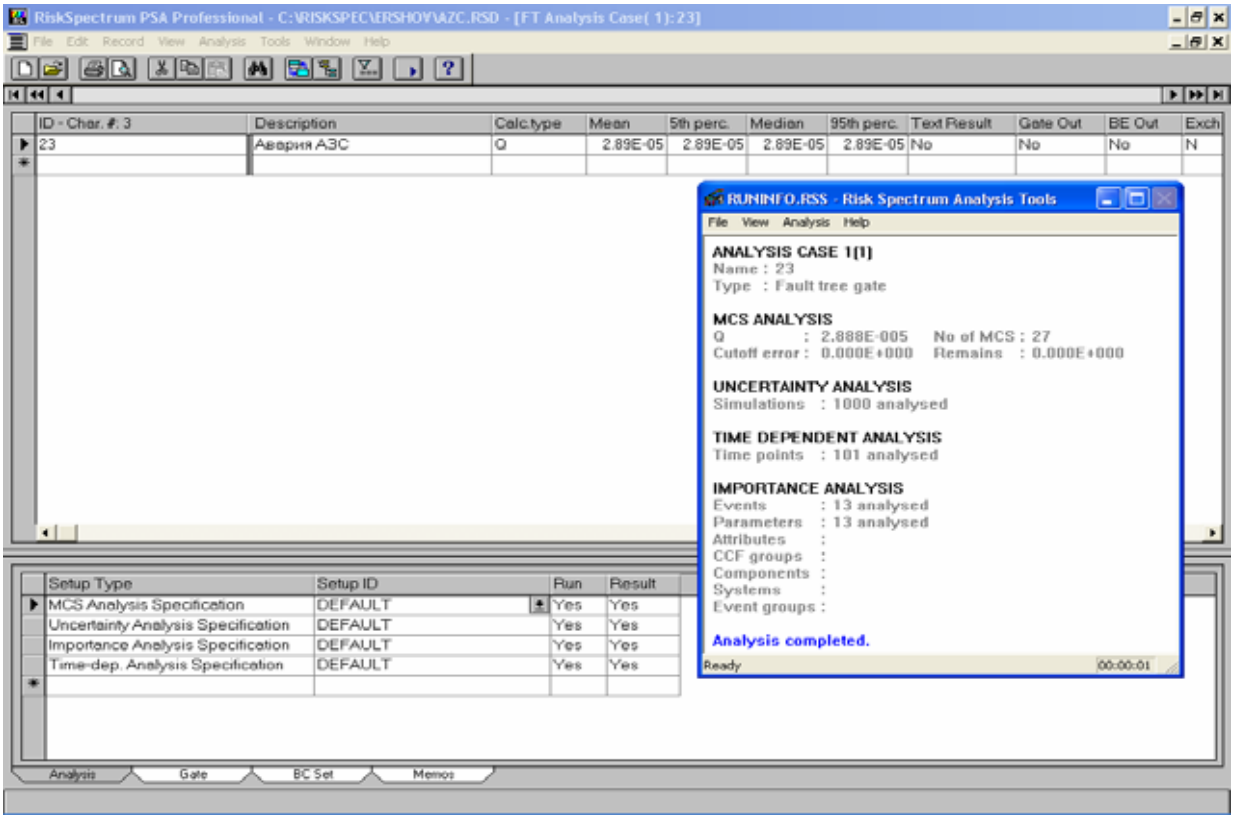
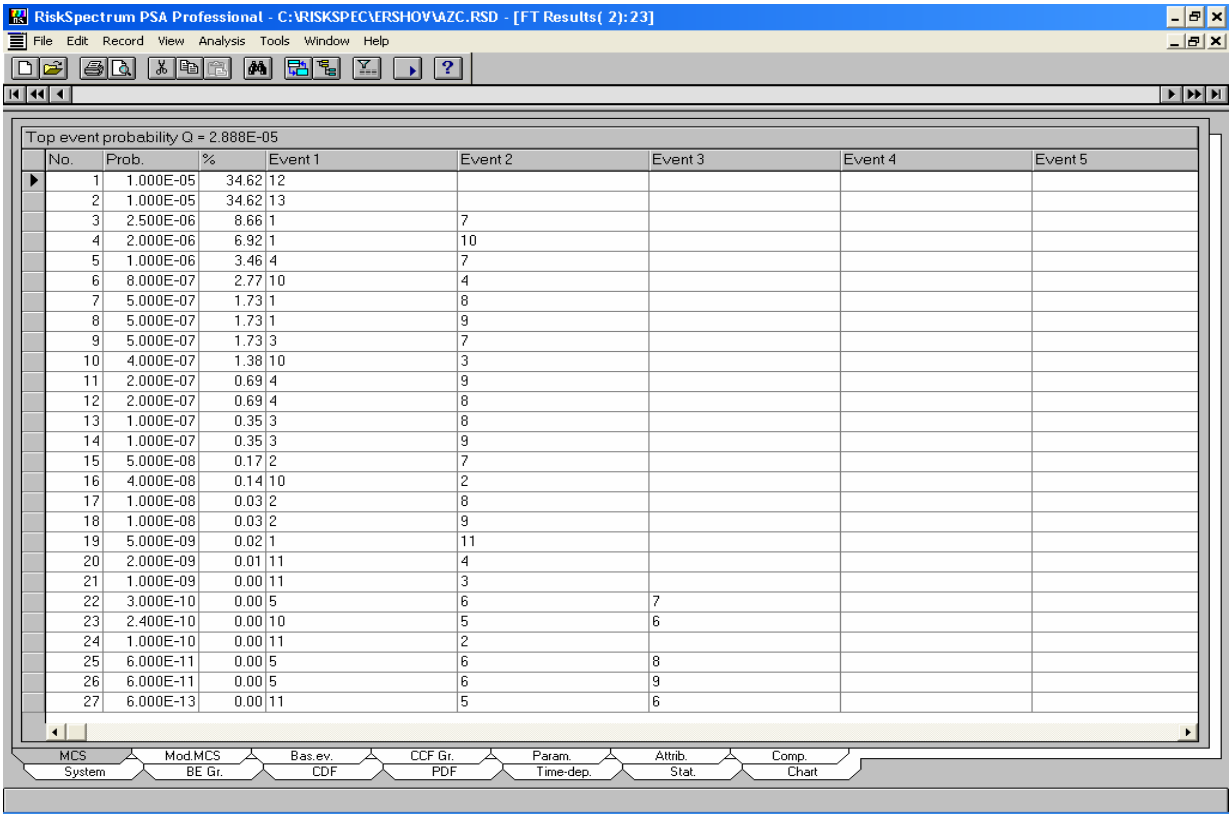


Рис. 2.12.10. Результаты расчетов вероятности аварии заправочной операции на ПК «Risk Spectrum»



No.	Prob.	%	Event 1	Event 2	Event 3	Event 4	Event 5
1	1.000E-05	34.62	12				
2	1.000E-05	34.62	13				
3	2.500E-06	8.66	1	7			
4	2.000E-06	6.92	1	10			
5	1.000E-06	3.46	4	7			
6	8.000E-07	2.77	10	4			
7	5.000E-07	1.73	1	8			
8	5.000E-07	1.73	1	9			
9	5.000E-07	1.73	3	7			
10	4.000E-07	1.38	10	3			
11	2.000E-07	0.69	4	9			
12	2.000E-07	0.69	4	8			
13	1.000E-07	0.35	3	8			
14	1.000E-07	0.35	3	9			
15	5.000E-08	0.17	2	7			
16	4.000E-08	0.14	10	2			
17	1.000E-08	0.03	2	8			
18	1.000E-08	0.03	2	9			
19	5.000E-09	0.02	1	11			
20	2.000E-09	0.01	11	4			
21	1.000E-09	0.00	11	3			
22	3.000E-10	0.00	5	6	7		
23	2.400E-10	0.00	10	5	6		
24	1.000E-10	0.00	11	2			
25	6.000E-11	0.00	5	6	8		
26	6.000E-11	0.00	5	6	9		
27	6.000E-13	0.00	11	5	6		

Рис. 2.12.11. Минимальные сечения отказов при аварии заправочной операции, полученные на ПК «Risk Spectrum»

Сводная таблица результатов раздела 2.12. " Анализ безопасности автоматизированной заправочной станции "			
Показатели безопасности АЗС	Результаты моделирования и расчетов		
	Relex Markov Relex Fault Tree Relex RBD	**ПК АСМ**	**Risk Spectrum**
1	**2**	**3**	**4**
Число конъюнкций логической модель возникновения аварии	***Логические модели совпали***		
	27	**27**	**27**
Вероятность возникновения аварии	Relex Fault Tree **0.00002888** Relex RBD **0.0000288849**	**0.000028884888**	**2.89E-5 = = 0.0000289**
Число конъюнкций логической модель отсутствия аварии	***Логические модели совпали***		
	3	**3**	**не определяются**
Вероятность отсутствия аварии	**0.99997112**	**0.999971115112**	

ВЫВОДЫ ПО РАЗДЕЛУ 2.12

Выводы специалистов ИПУ РАН

С классической логико-вероятностной задачей данного раздела все три комплекса успешно справились.

Выводы специалистов ОАО "СПИК СЗМА"

1. Средствами технологий АСМ и Relex данная задача двумя способами, на основе блок-схемы и дерева отказов. Средствами Risk Spectrum разработана обратная модель возникновения аварии с помощью дерева отказов.
2. Все результаты моделирования и расчетов совпали.

Выводы специалистов СПбАЭП

1. Результаты решения данной задачи всеми тремя комплексами одинаковы.

2. ПК Relex позволяет решить данную задачу, как на основе деревьев отказов, так и на основе блок-схем, генерировать как КПУФ, так и МСО.

3. ПК АСМ позволяет решать как прямую, так и обратную задачу по СФЦ «успеха» и по СФЦ «отказа», генерировать как КПУФ, так и МСО.

4. ПК Risk Spectrum позволяет решать только один вид задач по одной графической модели, генерировать только списки МСО.