



**НЕВА-ТОПМОНТАЖ-АВТОМАТИКА**

## **АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ НАДЕЖНОСТЬ И БЕЗОПАСНОСТЬ**

**АВТОМАТИЗИРОВАННОЕ СТРУКТУРНО-ЛОГИЧЕСКОЕ МОДЕЛИРОВАНИЕ И РАСЧЕТ  
НАДЕЖНОСТИ И БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ  
ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ И ОБОРУДОВАНИЕМ  
НА СТАДИИ ПРОЕКТИРОВАНИЯ**

Методические рекомендации

Санкт-Петербург

2003 г.

III

II

## АННОТАЦИЯ

1. Методические рекомендации разработаны по плану НИР на 2002 г. ОАО "Ассоциация "Монтажавтоматика" (Москва) в ОАО "Специализированная инжиниринговая компания "Севзапмонтажавтоматика" (Санкт-Петербург).

2. Методические рекомендации предназначены для специалистов предприятий и организации, выполняющих работы по моделированию и расчету показателей надежности и безопасности автоматизированных систем управления технологическими процессами и оборудованием на стадии проектирования. Сформулированы общие положения, цели и задачи Методических рекомендаций. Дана общая характеристика и порядок применения технологии и программных комплексов автоматизированного структурно-логического моделирования и расчета показателей надежности и безопасности АСУТП на стадии проектирования. Приведены примеры автоматизированного моделирования и расчета надежности и безопасности АСУТП.

3. Методические рекомендации разработаны под общей редакцией генерального директора ОАО "СПИК СЗМА" Нозика А.А.

4. Разработчик: ведущий специалист Научно-исследовательского отдела ОАО "СПИК СЗМА" д.т.н., профессор Можаяев А.С.

5. Методические рекомендации разработаны впервые.

## СОДЕРЖАНИЕ

1. ОБЛАСТЬ ПРИМЕНЕНИЯ .....	2
2. РУКОВОДЯЩИЕ И НОРМАТИВНЫЕ ДОКУМЕНТЫ.....	4
3. ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ.....	4
4. ЦЕЛИ И ЗАДАЧИ МЕТОДИЧЕСКИХ РЕКОМЕНДАЦИЙ.....	6
5. ОБЩАЯ ХАРАКТЕРИСТИКА ТЕХНОЛОГИИ АВТОМАТИЗИРОВАННОГО СТРУКТУРНО-ЛОГИЧЕСКОГО МОДЕЛИРОВАНИЯ.....	7
6. ПОРЯДОК ПРИМЕНЕНИЯ ТЕХНОЛОГИИ АСМ .....	9
6.1. Основные этапы технологии АСМ .....	9
6.2. Содержание и организация выполнения первого этапа постановки задачи автоматизированного моделирования и расчетов .....	10
6.3. Содержание и организация выполнения второго этапа автоматизированного моделирования и расчетов .....	11
6.4. Содержание и организация выполнения третьего этапа применения результатов автоматизированного моделирования и расчетов .....	12
7. ЛИТЕРАТУРА .....	13
Приложение 1. Аппарат схем функциональной целостности .....	14
Приложение 2. Состав модулей типового программного комплекса АСМ .....	16
Приложение 3. Методы расчета типовых вероятностных показателей надежности и безопасности АСУТП .....	19
Приложение 4. Примеры применения технологии АСМ .....	22
Пример 1. Автоматизированное моделирование и расчет надежности программно-логического контроллера АСУТП.....	22
Пример 2. Автоматизированное моделирование и расчет безопасности заправочной операции .....	32

## АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ НАДЕЖНОСТЬ И БЕЗОПАСНОСТЬ

### АВТОМАТИЗИРОВАННОЕ СТРУКТУРНО-ЛОГИЧЕСКОЕ МОДЕЛИРОВАНИЕ И РАСЧЕТ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ И ОБОРУДОВАНИЕМ НА СТАДИИ ПРОЕКТИРОВАНИЯ

#### Методические рекомендации

---

Дата введения

### 1. ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Настоящие Методические рекомендации (МР) предназначены для использования проектными организациями, проектными и проектно-конструкторскими отделами других организаций и предприятий (далее Предприятия), выполняющих работы по моделированию и расчету показателей надежности и безопасности автоматизированных систем управления технологическими процессами и оборудованием (АСУТП) на стадии проектирования.

1.2. Моделирование и расчет надежности и безопасности АСУТП выполняются при проектировании объектов нового строительства, реконструкции и технического перевооружения объектов производственного назначения:

- в безусловном порядке, когда их проведение регламентировано руководящими и нормативными документами Государственных надзорных органов;
- как правило, при создании АСУТП взрывопожароопасных и токсичных технологических установок, имеющих в своем составе блоки 1-й и 2 категории взрывоопасности, и других потенциально опасных объектов;
- при требованиях о выполнении расчетов надежности и безопасности, установленных заказчиками в заданиях на проектирование, технических заданиях на создание АСУТП, текстах контрактов (договоров).

1.3. В Методических рекомендациях излагаются основы современной технологии автоматизированного структурно-логического моделирования (АСМ) и расчета показателей надежности и безопасности структурно-сложных и высокоразмерных АСУТП, которая включает в себя:

- общий логико-вероятностный метод (ОЛВМ) анализа структурно-сложных систем;

- специализированные программные комплексы (ПК), в которых автоматизированы процессы построения логико-вероятностных моделей и расчета показателей надежности и безопасности структурно-сложных и высокоразмерных АСУТП;
- методики постановки задач, использования программных комплексов автоматизированного моделирования и применения результатов оценки надежности и безопасности АСУТП на стадии проектирования.

1.4. Автоматизированное структурно-логическое моделирование и расчет надежности и безопасности выполняются для оценки уровня безотказности и/или безопасности протекания технологических процессов (функционирования оборудования), как по отдельным функциям (подсистемам, контурам управления) и аварийным ситуациям, так и по проектируемой АСУТП в целом.

1.5. Результаты расчетов надежности и безопасности АСУТП предусмотрено использовать самостоятельно и как составную часть оценки риска аварий на опасных производственных объектах в соответствии с Методическими указаниями РД 03-418-01.

1.6. Результаты моделирования и расчетов надежности оформляются документом "Проектная оценка надежности системы", который разрабатывается в части проекта "Общесистемные решения". Состав и содержание документа должны соответствовать п.2.10 РД50-34.698-90.

1.7. Настоящие Методические рекомендации являются основой для разработки в ведомствах и на Предприятиях методических документов (отраслевых методических указаний, стандартов предприятий, рекомендаций, методик и т.п.) по внедрению и применению технологий автоматизированного моделирования и расчетов надежности и безопасности проектируемых АСУТП.

1.8. Методические рекомендации разработаны в соответствии с требованиями государственных и межотраслевых нормативно-технических документов, перечисленных в п.2.

1.9. При использовании иных технологий автоматизированного моделирования (например, деревьев отказов, деревьев событий и др.) для расчета показателей надежности и безопасности АСУТП, должны разрабатываться соответствующие методические рекомендации.

## 2. РУКОВОДЯЩИЕ И НОРМАТИВНЫЕ ДОКУМЕНТЫ

Настоящие Методические рекомендации разработаны на основе и в соответствии с требованиями следующих нормативно-технических документов:

- ГОСТ 27.001-95. Межгосударственный стандарт. Система стандартов "Надежность в технике". Основные положения. Минск: Межгосударственный совет по стандартизации, метрологии и сертификации, 1997. –3 с.
- ГОСТ 27.002-89 Надежность в технике. Основные понятия. Термины и определения. М.: Издательство стандартов, 1989.
- ГОСТ 27.301-95 Надежность в технике. Расчет надежности. Основные положения. М.: Изд-во стандартов, 1997. – 15 с.
- ГОСТ 24.701-86. Единая система стандартов автоматизированных систем управления. Надежность автоматизированных систем управления. Основные положения. М.: Издательство стандартов, 1987. – 17 с.
- ГОСТ 27.310-95. Межгосударственный стандарт. Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения. М.: Издательство стандартов, 1997. – 12 с.
- РД 03-418-01 Методические рекомендации по проведению анализа риска опасных производственных объектов. Документы межотраслевого применения по вопросам промышленной безопасности, охраны недр. Госгортехнадзор России, 2001. –20 с.
- ПБ 09-170-27 Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств. Утверждены постановлением Госгортехнадзора России от 22.12.97 г. №52.
- Общие правила взрывобезопасности химических производств и объектов. Утверждены Министерством по чрезвычайным ситуациям Республики Беларусь 28 июня 1996 г. Минск: 1996 г. - 80 с.
- РД 50-34.698-90 Методические указания. Информационная технология. Автоматизированные системы. Требования к содержанию документов. Государственный комитет СССР по управлению качеством продукции и стандартами. М.: Издательство стандартов, 1990, 38 с.

## 3. ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

3.1. В настоящем МР использованы термины и сокращения:

- по надежности в технике в соответствии с ГОСТ 27.001-95, ГОСТ 27.002-89, 27.301-95;
- по надежности систем автоматизации в соответствии с ГОСТ 24.701-86;
- по безопасности и риску в соответствии с ГОСТ 27.310-95, РД 03-418-01, ПБ 09-170-27.

3.2. Дополнительно в МР использованы следующие термины и сокращения:

АСУТП – автоматизированные системы управления технологическими процессами и оборудованием;

F – функция или множество главных функций, реализуемых АСУТП;

АС – аварийная ситуация или множество аварийных ситуаций, которые могут возникнуть в процессе функционирования проектируемой АСУТП;

ОЛВМ – общий логико-вероятностный метод теории автоматизированного структурно-логического моделирования систем;

АСМ – автоматизированное структурно-логическое моделирование – информационная технология, основанная на ОЛВМ, в которой строго формализованы и автоматизированы процессы построения математических моделей и расчетов показателей надежности и безопасности АСУТП большой размерности и высокой структурной сложности;

ПК АСМ – программный комплекс автоматизированного структурно-логического моделирования и расчета показателей надежности и безопасности АСУТП;

СФЦ – схема функциональной целостности проектируемой АСУТП или ее подсистемы, которая представляет собой специальный ориентированный граф  $G(X, Y)$ , где  $X$  – множество вершин, представляющих элементы, а  $Y$  – множество дуг, представляющих логические связи между элементами в АСУТП;

ЛКФ – логический критерий функционирования, определяющий условие реализации выходной функции  $F$  или возникновения аварийной ситуации  $АС$  в проектируемой АСУТП;

ФРС – логическая функция работоспособности системы;

КПУФ – кратчайшие пути успешного функционирования;

МСО – минимальные сечения отказов;

ВФ – вероятностная функция (многочлен);

ПЛК – программно-логический контроллер;

Показатели безопасности – вероятностные и другие характеристики возникновения аварийной ситуации в АСУТП вследствие отказов ее элементов и других факторов;

Предприятия - проектные организации, проектные и проектно-конструкторские отделы других организаций и предприятий, в интересах которых выполняются (самостоятельно или по заказу) работы по оценке надежности и безопасности АСУТП строящихся, реконструируемых или модернизируемых объектов;

Исполнитель – организации, их структурные подразделения и специалисты, выполняющие автоматизированное структурно-логическое моделирование и расчет показателей надежности и безопасности АСУТП;

Заказчик – организации, их структурные подразделения и специалисты, в интересах которых Исполнитель выполняет моделирование и расчет надежности и безопасности АСУТП. В частности, Заказчиком может быть разработчик АСУТП.

#### **4. ЦЕЛИ И ЗАДАЧИ МЕТОДИЧЕСКИХ РЕКОМЕНДАЦИЙ**

4.1. Основной целью разработки Методических рекомендаций является реализация на Предприятиях требований государственных нормативных документов, указанных в п.2, по оценке надежности и безопасности АСУТП на стадии проектирования.

4.2. Основными задачами применения технологии автоматизированного структурно-логического моделирования и расчета надежности и безопасности АСУТП на стадии проектирования являются:

- определение достигнутого (ожидаемого) уровня надежности и безопасности АСУТП и их составных частей;
- сравнительный анализ структурных решений АСУТП и обоснование выбора оптимальных вариантов по критериям надежности, безопасности и стоимости;
- проверка соответствия ожидаемого (достигнутого) уровня надежности и безопасности проектируемых АСУТП требованиям нормативных документов, программ обеспечения надежности, технических заданий или контрактов (договоров);
- предоставление специалистам, разрабатывающим технические решения, объективной информации о состоянии системы, наиболее слабых (опасных) элементах (узлах, компонентах) и рекомендаций по увеличению надежности и безопасности АСУТП;
- повышение качества, конкурентоспособности и эффективности проектируемых АСУТП.

## 5. ОБЩАЯ ХАРАКТЕРИСТИКА ТЕХНОЛОГИИ АВТОМАТИЗИРОВАННОГО СТРУКТУРНО-ЛОГИЧЕСКОГО МОДЕЛИРОВАНИЯ

5.1. Существующие технологии моделирования и расчета надежности и безопасности структурно-сложных систем характеризуются следующими тремя основными этапами:

- постановки задачи, главное место в которой занимает разработка структурных схем надежности и/или сценариев возникновения аварийных ситуаций;
- построения расчетных математических моделей (логических, аналитических или статистических) для количественной оценки свойств надежности и безопасности систем;
- выполнения расчетов показателей надежности и безопасности систем и использование полученных результатов для выработки и обоснования исследовательских, проектных, эксплуатационных и других управленческих решений.

5.2. Постоянно возрастающие структурная сложность и размерность современных АСУТП сделали практически невозможным выполнение второго этапа средствами традиционных ("ручных") технологий построения математических моделей их надежности и безопасности. Решить данную проблему предусмотрено на основе технологий, в которых автоматизированы процессы построения сложных и высокоразмерных математических моделей надежности и безопасности АСУТП.

5.3. Существующие отечественные и зарубежные технологии и программные комплексы автоматизированного моделирования различаются способами представления исходных структурных схем, предметными областями (классами анализируемых объектов), методами и программными комплексами автоматизированного моделирования, а также составом вычисляемых показателей надежности и безопасности исследуемых систем. В настоящее время наибольшее распространение получили технологии автоматизированного моделирования, в основе которых лежат способы построения структурных схем надежности и сценариев возникновения аварий в виде деревьев отказов, деревьев событий, схем последовательно-параллельного соединения элементов, графов связности и схем функциональной целостности. Теоретической основой указанных технологий выступают различные модификации так называемых логико-вероятностных методов исследования надежности структурно-сложных систем. По специализации, уровню теоретической разработки, качеству программной реализации, а также составу и точности вычисления показателей, разные технологии автоматизированного моделирования могут существенно отличаться друг от друга и в различной степени удовлетворять целям, задачам и особенностям проектных расчетов надежности и безопасности АСУТП различных типов и назначения.

5.4. Рассматриваемая в настоящих Методических рекомендациях технология автоматизированного структурно-логического моделирования и расчета показателей надежности и безопасности АСУТП на стадии проектирования характеризуется следующими основными положениями:

5.4.1. В технологии АСМ используется универсальный графический аппарат построения структурных моделей на этапе постановки задач оценки надежности и безопасности АСУТП – схемы функциональной целостности (СФЦ). С помощью СФЦ могут представляться практически все известные структурные схемы надежности и безопасности систем, используемые в других технологиях автоматизированного моделирования (деревья отказов, деревья событий, последовательно-параллельные соединения, графы связности и др.). Вместе с тем аппарат СФЦ позволяет строить принципиально новые классы немонотонных и комбинаторно-последовательных структурных моделей надежности и безопасности современных АСУТП.

5.4.2. Теоретической основой технологии АСМ является общий логико-вероятностный метод (ОЛВМ) системного анализа. В сравнении с другими структурными методами моделирования надежности и безопасности систем, ОЛВМ впервые реализует все возможности основного аппарата моделирования – алгебры логики в базисе функционально полного набора операций "И", "ИЛИ" и "НЕ". Это позволяет с помощью ОЛВМ решать задачи оценки надежности и безопасности, которые решаются методами других технологий автоматизированного моделирования, а также учитывать в формируемых моделях ряд новых системных особенностей современных АСУТП.

5.4.3. В ОЛВМ полностью алгоритмизированы и реализованы в программных комплексах автоматизированного структурно-логического моделирования (ПК АСМ) наиболее сложные и громоздкие процессы построения математических моделей и выполнения расчетов показателей надежности и безопасности АСУТП. Это позволяет, во-первых, оценивать надежность и безопасность АСУТП большой размерности и высокой структурной сложности, и, во-вторых, осуществить практическое внедрение технологии автоматизированного структурно-логического моделирования в деятельность Предприятий.

5.4.4. Универсальность и полнота разработки ОЛВМ обеспечивают возможность дальнейшего развития технологии и ПК АСМ, а также их адаптацию к особенностям задач моделирования и расчета надежности и безопасности АСУТП различных Предприятий.

## 6. ПОРЯДОК ПРИМЕНЕНИЯ ТЕХНОЛОГИИ АСМ

### 6.1. Основные этапы технологии АСМ

6.1.1. На первом этапе постановки задачи осуществляется:

- составление перечней главных функций  $F$  проектируемой АСУТП и возможных аварийных ситуаций  $АС$ , вероятностных и других системных показателей надежности и безопасности, которые должны быть определены в процессе моделирования и расчетов;
- построение формализованных структурных моделей (схем, сценариев) надежности и безопасности проектируемой АСУТП и определение критериев реализации главных функций ( $F$ ) и возникновения аварийных ситуаций ( $АС$ ).
- определение вероятностных и других параметров надежности элементов АСУТП и событий (нежелательных, инициирующих и др.), определяющих условия возникновения аварийных ситуаций.

По составу, содержанию и форме представления исходные данные, определяемые на первом этапе, должны позволять использовать соответствующие программные комплексы на следующих этапах автоматизированного структурно-логического моделирования и расчета надежности и безопасности АСУТП.

6.1.2. На втором этапе автоматизированного моделирования и расчетов выполняется:

- ввод исходных данных (схем функциональной целостности, критериев функционирования, параметров элементов и др.) в ПК АСМ;
- автоматическое построение математических моделей (логических, аналитических, статистических, марковских или др.) и расчеты на их основе показателей надежности и безопасности проектируемой АСУТП.

6.1.3. На третьем этапе применения результатов осуществляется выработка и обоснование проектных (управленческих) решений путем:

- использования вычисленных вероятностных показателей надежности и безопасности проектируемой АСУТП;
- детерминированного анализа отказоустойчивости и безопасности АСУТП на основе логических моделей реализации функций и возникновения аварийных ситуаций;
- решения задач параметрической и структурной оптимизации проектируемых АСУТП.

Содержание и организация выполнения указанных этапов технологии автоматизированного структурно-логического моделирования и расчета показателей надежности и безопасности АСУТП описаны в п.п.6.2 – 6.4 настоящих МР.

## **6.2. Содержание и организация выполнения первого этапа постановки задачи автоматизированного моделирования и расчетов**

6.2.1. Для эффективного применения технологии автоматизированного структурно-логического моделирования на Предприятиях необходимо обеспечить методическую подготовку и организацию эффективной совместной работы специалистов по проектированию АСУТП, в интересах которых производится оценка надежности и безопасности (Заказчика), и специалистов по применению технологии и программных комплексов автоматизированного структурно-логического моделирования (Исполнителя).

6.2.2. Начальный этап и основную, содержательную часть постановки задачи выполняет Заказчик, или привлеченная им для участия в работе специализированная организация (специалисты). На этом этапе выполняется подготовка исходных данных, перечисленных в п. 6.1.1. При этом первичное представление структурных моделей АСУТП по функциям  $F$  и заданным аварийным ситуациям  $AC$  может осуществляться в любой из следующих общепринятых форм:

- структурно-функциональных схем с дополнительными описаниями логических условий работы элементов, реализации функций и возникновения аварийных ситуаций в АСУТП;
- деревьев отказов;
- деревьев событий;
- схем последовательно-параллельного соединения элементов;
- графов связности;
- схем функциональной целостности, которые непосредственно используются в технологии и ПК АСМ.

6.2.3. Значения исходных вероятностных  $p_i = p_i(t)$ ,  $q_i = 1 - p_i$ , и других параметров элементов  $i = 1, 2, \dots, N$  определяются в соответствии с ГОСТ 27.301-95. При этом источниками этих исходных данных могут быть:

- стандарты и технические условия на составные части и комплектующие элементы АСУТП;
- справочники и базы данных по надежности элементов и частотам нежелательных, инициирующих и др. исходных событий аварий АСУТП;
- данные о надежности объектов-аналогов элементов, входящих в состав АСУТП;
- другие источники, включая результаты обработки статистических данных эксплуатации, автономное моделирование и расчет надежности элементов и подсистем, а также экспертные оценки специалистов.

6.2.4. Завершающий этап постановки задачи выполняет Исполнитель. Он осуществляет формализацию исходных данных и подготовку их к вводу в ПК АСМ. В том случае, если структурные схемы АСУТП представлены Заказчиком не непосредственно в форме СФЦ, то Исполнитель преобразует их в графы  $G(X, Y)$  схем функциональной целостности и согласует с Заказчиком. Для каждой выходной функции из множества  $F$  и аварийной ситуации из множества  $AC$  формулируются соответствующие логические критерии функционирования  $Y_F(\{y_i\})$  и  $Y_{AC}(\{y_i\})$ .

Изобразительные средства и методика построения СФЦ изложены в Приложении 1. Примеры формализованной постановки задачи автоматизированного структурно-логического моделирования фрагментов АСУТП приведены в Приложении 4.

6.2.5. Работы по первому этапу постановки задачи автоматизированного моделирования и расчетов могут выполняться Заказчиком, Исполнителем или совместно.

### **6.3. Содержание и организация выполнения второго этапа автоматизированного моделирования и расчетов**

6.3.1. Подготовленные на первом этапе формализованные исходные данные (СФЦ, ЛКФ и параметры элементов) для каждой выходной функции  $F$  и заданной аварийной ситуации  $AC$  Исполнитель вводит в ПК АСМ. В Приложении 2 описан состав модулей типового программного комплекса автоматизированного структурно-логического моделирования надежности и безопасности АСУТП.

6.3.2. На основе введенного в ПК АСМ графа  $G(X, Y)$  СФЦ проектируемой АСУТП для каждого заданного ЛКФ  $Y_F(\{y_i\})$ ,  $Y_{AC}(\{y_i\})$  осуществляется автоматическое построение логических функций работоспособности  $Y_F(\{x_i\})$  и  $Y_{AC}(\{x_i\})$ . Автоматическое построение ФРС осуществляется в ПК АСМ универсальным программным модулем логического моделирования. Он позволяет получать все возможные виды логических ФРС, например, кратчайшие пути успешного функционирования, минимальные сечения отказов, минимальные пропускные и отсекающие сочетания, а также их немонотонные комбинации.

6.3.3. Полученные логические ФРС  $Y_F(\{x_i\})$  и  $Y_{AC}(\{x_i\})$  с помощью программных комплексов аналитического моделирования автоматически преобразуются в соответствующие многочлены расчетных вероятностных функции  $P_F(\{p_i, q_i, t\})$  и  $P_{AC}(\{p_i, q_i, t\})$ . Многочлены ВФ являются аналитическими законами распределения времени безотказной работы, которые соответствуют СФЦ и заданным логическим критериям функционирования АСУТП.

6.3.4. С помощью полученных логических и вероятностных математических моделей в ПК АСМ выполняются расчеты требуемых показателей надежности и безопасности проектируемых АСУТП. В Приложении 3 описаны ряд методов расчета типовых показателей надежности АСУТП, которые реализованы в базовых образцах ПК АСМ. В Приложении 4 приведены два примера расчета вероятностных показателей и детерминированного анализа надежности и безопасности фрагментов АСУТП.

6.3.5. Состав методов и методики расчета, вероятностных и других показателей надежности и безопасности, могут изменяться в процессе развития теории и адаптации технологии и программных комплексов автоматизированного структурно-логического моделирования АСУТП к особенностям различных Предприятий.

#### ***6.4. Содержание и организация выполнения третьего этапа применения результатов автоматизированного моделирования и расчетов***

6.4.1. Для выработки и принятия проектных решений на основе результатов автоматизированного моделирования, на Предприятиях используются типовые или специально разрабатываемые методы, компьютерные программы и методики, позволяющие реализовать цели и решать задачи расчета надежности и безопасности АСУТП. В этих методах должны учитываться особенности проектируемых на Предприятиях АСУТП и объектов управления.

6.4.2. Одним из типовых приемов использования результатов автоматизированного моделирования и расчетов является нормативный анализ. Он осуществляется путем сравнения показателей достигнутого уровня надежности и безопасности проектируемой АСУТП с требованиями, указанными в нормативных документах, технических заданиях или программах обеспечения надежности. По результатам нормативного анализа принимаются соответствующие проектные и другие решения.

6.4.3. Использование результатов автоматизированного моделирования в процессе проектирования должно осуществляться на основе объективной оценки роли (значимости, положительных и отрицательных вкладов) отдельных или групп элементов в обеспечение надежности и безопасности АСУТП в целом. На этой основе вырабатываются оптимальные, по технико-экономическим показателям, проектные решения, направленные на увеличение надежности, безопасности, эффективности и снижение риска функционирования разрабатываемых АСУТП. Пример использования результатов автоматизированного моделирования и расчетов для увеличения надежности и безопасности фрагмента АСУТП приведен в Приложении 4.

6.4.4. Рекомендуется планировать работы, направленные на совершенствование и адаптацию технологии и ПК АСМ к особенностям различных Предприятий, разработку методов, компьютерных программ и методик применения результатов моделирования и оценки надежности и безопасности для выработки и обоснования проектных (управленческих) решений.

## 7. ЛИТЕРАТУРА

1. Рябинин И.А., Черкесов Г.Н. Логико-вероятностные методы исследования надежности структурно-сложных систем. М.: Радио и связь, 1981.
2. Рябинин И.А. Надежность и безопасность сложных систем. СПб.: Политехника, 2000.
3. Дж.Хенли, Х.Кумамото. Надежность технических систем и оценка риска. М.: Машиностроение, 1984.
4. Можаяев А.С. Теория и практика автоматизированного структурно-логического моделирования систем. // Доклады международной конференции по информатике и управлению. (ICI & C') Том 3. СПб.: СПИИРАН, 1997, с.1109-1118.
5. Можаяев А.С. Программный комплекс автоматизированного структурно-логического моделирования сложных систем (ПК АСМ 2001). // Труды Международной Научной Школы 'Моделирование и анализ безопасности, риска и качества в сложных системах' (МА БРК – 2001). СПб.: Издательство ООО 'НПО 'Омега', 2001, с.56-61.
6. Нозик А.А. Технология автоматизированного структурно-логического моделирования в проектных расчетах надежности систем. // Труды второй международной научной школы "Моделирование и анализ безопасности и риска в сложных системах". МА БР - 2002. СПб.: Издательство "Бизнес-Пресса", 2002, - с. 337-344.
7. Нозик А.А. Методы проектного расчета надежности автоматизированных систем управления технологическими процессами. // Труды II международной научно-практической конференции. Часть I. "Микропроцессорные, аналоговые и цифровые системы: проектирование и системотехника, теория и вопросы применения". Новочеркасск: НПИ, 20002, -с.33-45.
8. Проурзин В.А. Алгоритмы численного анализа надежности и риска для сложной системы на основе деревьев отказов. // Труды Международной Научной Школы 'Моделирование и анализ безопасности, риска и качества в сложных системах' (МА БРК – 2001). СПб.: Издательство ООО 'НПО 'Омега', 2001, с.263-268.

## АППАРАТ СХЕМ ФУНКЦИОНАЛЬНОЙ ЦЕЛОСТНОСТИ

### Изобразительные средства схем функциональной целостности



### Простейшие фрагменты схем функциональной целостности

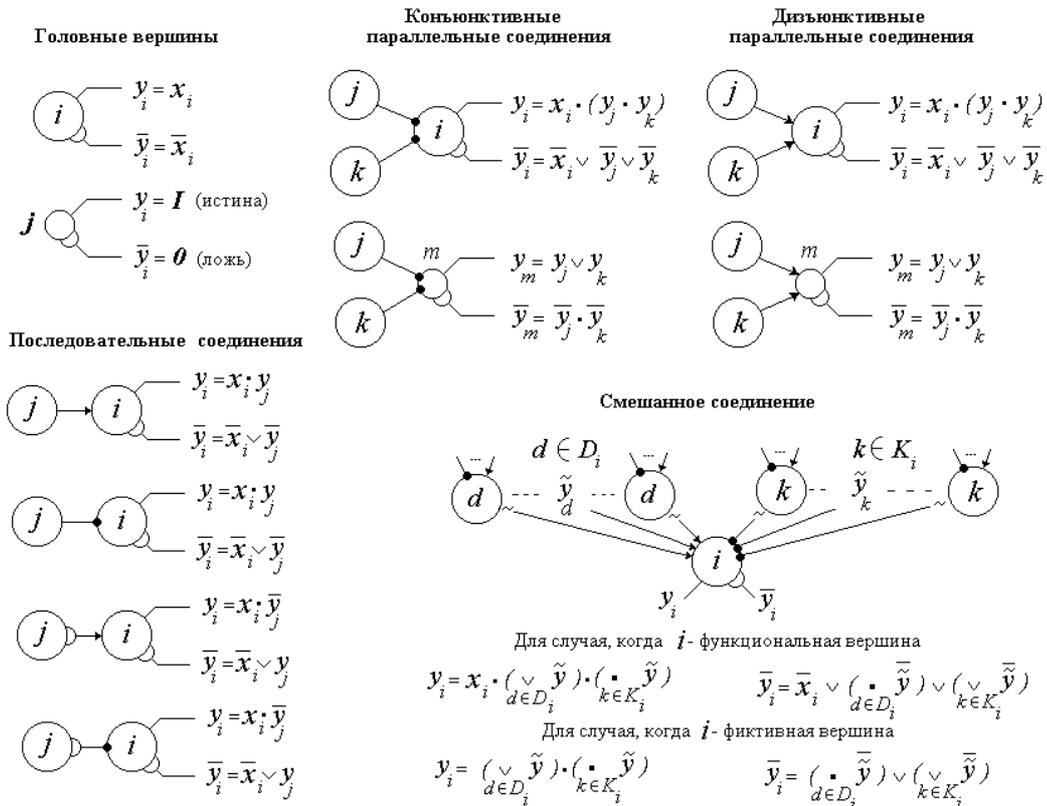


Рис. 1. Изобразительные средства и типовые фрагменты СФЦ

Разработка СФЦ для автоматизированного моделирования и расчета надежности и безопасности АСУТП является основой формализованной постановки задач в технологии АСМ. Теоретической базой методики разработки СФЦ и задания ЛКФ выступает общий логико-вероятностный метод системного анализа. Граф схемы функциональной целостности  $G(X, Y)$  представляет собой универсальное средство структурного представления состава элементов системы ( $x_i \in X$ ) и логических условий ( $y_i \in Y$ ) реализации ими своих функций в системе. С помощью логических критериев функционирования  $Y_F(\{y_i\})$  и  $Y_{AC}(\{y_i\})$  задаются условия реализации выходных функций ( $F$ ) и возникновения аварийных ситуаций ( $AC$ ) в проектируемой АСУТП.

Общая методика построения СФЦ включает в себя следующие основные этапы.

### **1) Подготовительный этап:**

- На основе предоставленных Заказчиком перечня элементов, форм представления и описания структурных схем АСУТП (см. п.6.2.2) определяется состав функциональных вершин  $i = 1, 2, \dots, N$ , которыми представляются в СФЦ элементы, входящие в структурные части (подсистемы) проектируемой АСУТП;

- На основе перечней и описаний функций  $F$  и аварийных ситуаций  $AC$  проектируемой АСУТП выделяются те ее структурные части (фрагменты и подсистемы), для которых должны быть построены частные СФЦ фрагментов и подсистем проектируемой АСУТП.

### **2) Разработка частных СФЦ фрагментов и подсистем АСУТП:**

- Для каждого элемента  $i$  фрагмента или подсистемы определяются его выходная функция  $y_i$ , и логические условия ее реализации функциями  $y_j, y_k, \dots$  других элементов данной структурной части АСУТП;

- Логические условия реализации выходных функций представляются графическими средствами СФЦ (см. рис.1) на входах и выходах функциональных и фиктивных вершин, входящих в состав разрабатываемых частных СФЦ фрагментов и подсистем проектируемой АСУТП.

### **3) Разработка общих СФЦ надежности и безопасности АСУТП и определение ЛКФ:**

- Сложные и высокоразмерные АСУТП могут представляться несколькими частными СФЦ надежности и безопасности отдельных и групп выходных функций  $F$  и аварийных ситуаций  $AC$  проектируемой АСУТП.

- При необходимости, разработанные СФЦ структурных фрагментов могут объединяться в общие СФЦ реализации всех выходных функций  $F$  и СФЦ возникновения аварийных ситуаций  $AC$  в проектируемой АСУТП.;

- Для каждой функции  $F$  и аварийной ситуации  $AC$  определяются (задаются) логически критерии функционирования  $Y_F(\{y_i\})$  и  $Y_{AC}(\{y_i\})$ . В технологии АСМ эти критерии могут определять, как условия реализации, так и условия не реализации функций  $F$  и аварийных ситуаций  $AC$ , а также любые немонотонные комбинации этих условий.

### **4) Анализ результатов построения СФЦ :**

- в случае согласования результатов структурного моделирования Заказчиком и Исполнителем, процедура построения СФЦ завершается;

- в противном случае выполняется итерационная корректировка предыдущих этапов до успешного построения СФЦ надежности и/или безопасности проектируемой АСУТП.

## СОСТАВ МОДУЛЕЙ ТИПОВОГО ПРОГРАММНОГО КОМПЛЕКСА АВТОМАТИЗИРОВАННОГО СТРУКТУРНО-ЛОГИЧЕСКОГО МОДЕЛИРОВАНИЯ

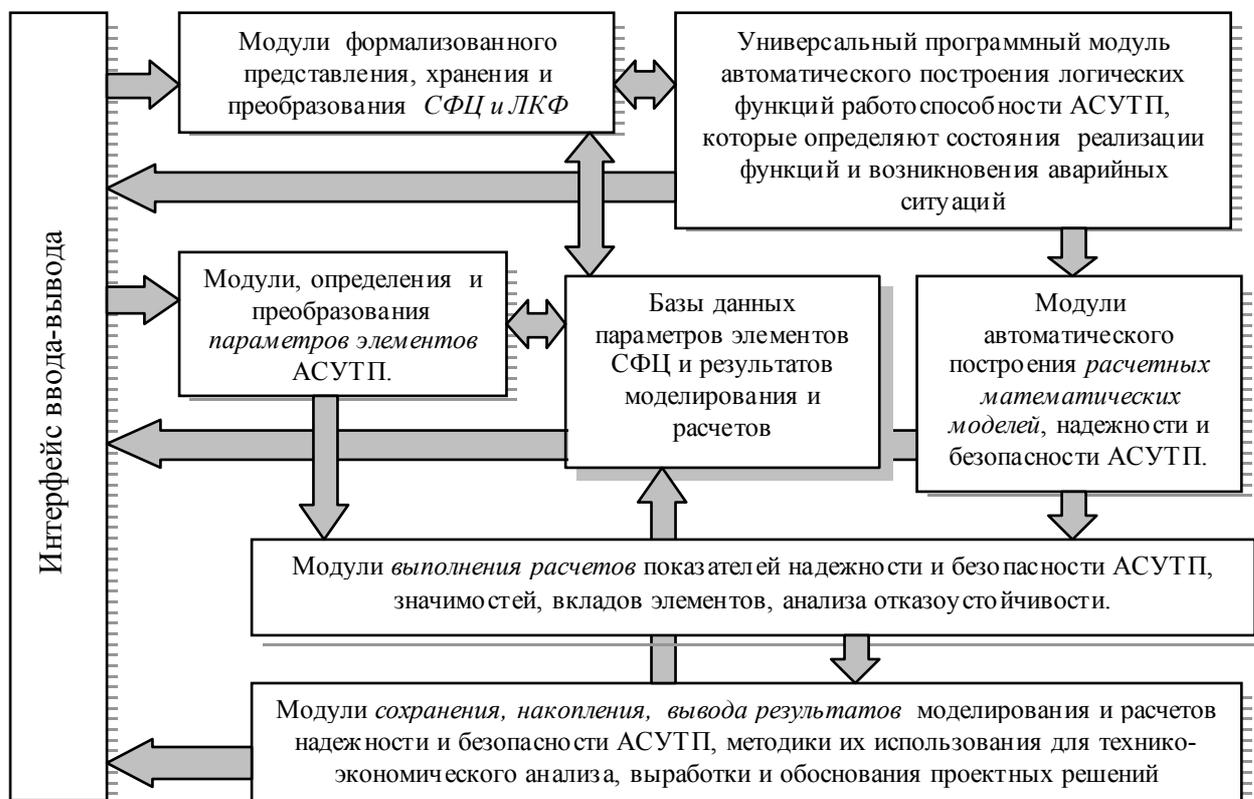


Рис.2. Структура и состав модулей типового ПК АСМ

1. Программные комплексы АСМ, используемые для моделирования и расчета надежности и безопасности АСУТП, по составу определяемых показателей и точности их вычислений должны соответствовать требованиям государственных и отраслевых нормативных и технических документов на создание АСУТП.

2. Схема, приведенная на рис.2, представляет базовый образец программного комплекса, реализующего технологию автоматизированного структурно-логического моделирования и расчета показателей надежности и безопасности АСУТП на стадии проектирования, который должен обладать следующими функциональными возможностями:

- выполнять автоматизированное моделирование и расчет показателей надежности и безопасности фрагментов, подсистем и АСУТП в целом, условия реализации функций и возникновения аварийных ситуаций в которых представлены графами схем функциональной целостности и логическими критериями функционирования;

- автоматически строить логические и вероятностные модели для АСУТП большой размерности и высокой структурной сложности;
- автоматически вычислять показатели надежности и безопасности АСУТП;
- обеспечивать возможность применения результатов моделирования и расчетов для выработки и технико-экономического обоснования проектных решений в области надежности и безопасности АСУТП на стадии проектирования.

3. Интерфейс ввода-вывода ПК АСМ должен обеспечивать удобный (как правило, графический) ввод исходных данных (СФЦ, ЛКФ, параметров элементов и режимов работы ПК АСМ) и вывод результатов моделирования и расчетов показателей надежности и безопасности АСУТП.

4. Модули формализованного представления, хранения и преобразования СФЦ и ЛКФ предназначены для обеспечения эффективной обработки в ПК АСМ структурных моделей надежности и безопасности АСУТП большой размерности и высокой структурной сложности. В частности, они должны обеспечивать реализацию процессов декомпозиции и агрегирования громоздких процедур автоматического построения логических ФРС.

5. Универсальная программа (программный модуль) построения логических функций работоспособности является центральным звеном ПК АСМ. Она должна позволять автоматически формировать различные виды логических ФРС: монотонных (в базисе операций "И", "ИЛИ") и немонотонных (в базисе операций "И", "ИЛИ", "НЕ"), КПУФ, МСО, минимальных пропускных и отсечных сочетаний, а также любые их комбинации. В логических ФРС должны учитываться особенности различных АСУТП. Например, разные начальные состояния системы, наличие группы несовместных событий, отказы по общей причине, многофункциональность элементов, наличие элементов с числом состояний больше двух, способность АСУТП функционировать в различных состояниях с разной эффективностью или различной степенью риска, и др.

6. Модули определения и преобразования параметров элементов должны осуществлять оперативную подготовку исходных данных для выполнения расчетов показателей надежности и безопасности АСУТП.

7. Базы данных, входящие в состав или связанные с ПК АСМ, должны обеспечивать выдачу, хранение и обновление параметров элементов, типовых фрагментов и ранее подготовленных СФЦ, а также результатов автоматизированного моделирования и расчетов надежности и безопасности АСУТП.

8. Программные модули автоматического построения расчетных математических моделей в зависимости от специализации ПК АСМ должны выполнять:

- формирование аналитических моделей в виде многочленов расчетных вероятностных и других функций (реализуется в базовом образце ПК АСМ);
- формирование статистических моделей оценки показателей надежности и безопасности АСУТП;
- формирование марковских моделей для динамического анализа надежности и безопасности АСУТП;
- формирование различных сетевых моделей функционирования АСУТП, позволяющих учесть, например, последовательности отказов элементов, влияние ненадежных переключателей и процессов развития возможных аварийных ситуаций.

9. Модули выполнения расчетов предназначены для количественной оценки различных единичных и комплексных показателей надежности и безопасности АСУТП, относящихся к объектам I и II вида (по классификации ГОСТ 27.301). Одновременно с расчетом общесистемных показателей в ПК АСМ должны определяться характеристики роли отдельных элементов (значимостей и вкладов). Это обеспечит возможность дальнейшей автоматизации процессов решения специальных задач технико-экономического обоснования, оптимизации, распределения ресурсов, целевого планирования и управления разработкой АСУТП на стадии проектирования.

10. Модули сохранения, накопления и вывода результатов предназначены для обеспечения удобной и эффективной работы лиц, принимающих проектные решения, и реализации различных методик технико-экономического обоснования проектируемых АСУТП.

11. Структура и программная реализация комплексов АСМ должны обеспечивать возможность их дальнейшего совершенствования, развития а адаптацию к особенностям решения задач оценки надежности и безопасности АСУТП различных Предприятий.

### МЕТОДЫ РАСЧЕТА ТИПОВЫХ ВЕРОЯТНОСТНЫХ ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ АСУТП

1. Вероятности  $P_F(t)$  безотказной работы (или отказа) и  $P_{AC}(t)$  возникновения (или не возникновения) аварийных ситуаций для невосстанавливаемых АСУТП рассчитываются путем подстановки в соответствующие многочлены  $P_F(\{p_i, q_i, t\})$  и  $P_{AC}(\{p_i, q_i, t\})$  числовых значений вероятностей безотказной работы и/или отказа элементов  $p_i = p_i(t)$ ,  $q_i = 1 - p_i$ . При экспоненциальном законе распределения наработки до отказа, указанные вероятностные параметры элементов вычисляются по формулам:

$$\begin{aligned} p_i &= p_i(t) = e^{-\frac{t}{T_{oi}}}, \\ q_i &= q_i(t) = 1 - p_i(t), \end{aligned} \quad (1)$$

где  $i$  - номер элемента,  $T_{oi}$  - средняя наработка элемента до отказа,  $t$  - заданная наработка. Допускается использование других законов распределений или заданных (предварительно вычисленных) статических вероятностей  $p_i$ ,  $q_i = 1 - p_i$  элементарных событий моделей надежности и безопасности АСУТП.

2. Средняя наработка до отказа  $T_{OF}$  или аварии  $T_{OAC}$  невосстанавливаемой АСУТП определяются на основе следующей расчетной процедуры:

$$T_{OF/OAC} = \int_0^{\infty} P_{F/AC}(t) dt = \sum_{j=1}^M (zn_j) \frac{1}{\sum_{i \in K_j} \frac{1}{T_{oi}}} \quad (2)$$

где  $M$  - число одночленов в многочлене ВФ,  $(zn_j)$  - знак  $j$ -го одночлена ВФ, а  $K_j$  - множество номеров элементов, параметры  $p_i(t)$  которых вошли в состав  $j$ -го одночлена вероятностной функции.

3. Коэффициент готовности  $P_{F/AC}(t) = P_{F/AC} = K\Gamma_{F/AC}$  восстанавливаемой АСУТП рассчитывается путем подстановки в многочлены  $P_F(\{p_i, q_i, t\})$  или  $P_{AC}(\{p_i, q_i, t\})$  числовых значений коэффициентов готовности  $K\Gamma_i$  и коэффициентов неготовности  $1 - K\Gamma_i$  элементов:

$$p_i = K\Gamma_i = \frac{T_{oi}}{T_{oi} + T_{ei}}; \quad q_i = 1 - K\Gamma_i, \quad (3)$$

где  $T_{bi}$  - среднее время восстановления элемента.

4. В технологии АСМ предусмотрены расчеты трех видов показателей роли отдельных элементов в обеспечении надежности или безопасности АСУТП:

$$\text{Значимость элемента: } \xi_i = \left( P_{F/AC}(t) \Big|_{p_i(t)=1} \right) - \left( P_{F/AC}(t) \Big|_{p_i(t)=0} \right) \quad (4)$$

$$\text{Положительный вклад элемента: } B_i^+ = \left( P_{F/AC}(t) \Big|_{p_i(t)=1} \right) - P_{F/AC}(t) \quad (5)$$

$$\text{Отрицательный вклад элемента: } B_i^- = - \left( P_{F/AC}(t) - \left( P_{F/AC}(t) \Big|_{p_i(t)=0} \right) \right) \quad (6)$$

Здесь  $P_{F/AC}(t) \Big|_{p_i(t)=1}$  - значение вероятностной характеристики надежности или безопасности АСУТП при абсолютной надежности элемента  $i$ , а  $P_{F/AC}(t) \Big|_{p_i(t)=0}$  - значение той же характеристики АСУТП при достоверном отказе элемента  $i$  на рассматриваемом интервале  $t$  времени функционирования. Согласно (4) величина значимости  $\xi_i$  равна абсолютному изменению значения системной характеристики  $P_{F/AC}(t)$ , которое произойдет, если значение собственного параметра надежности элемента  $p_i = p_i(t)$  изменить от 0 до 1 включительно (при фиксированных значениях заданных параметров всех других элементов системы). Диапазон значений значимости в общем случае составляет  $[-1, 0, +1]$ . При этом  $\xi_i < 0$  означает, что увеличение надежности элемента уменьшает надежность всей системы (вредный, опасный элемент). Отрицательные значимости элементов характерны для немонотонных логико-вероятностных моделей АСУТП. Нулевые значимости  $\xi_i = 0$  имеют элементы, которые не участвуют в реализации функции  $F$  или аварийной ситуации  $AC$  (несущественные элементы). Положительные значимости  $\xi_i > 0$  определяют то максимально возможное увеличение характеристики  $P_{F/AC}(t)$  АСУТП, которое она может получить, если изменить надежность  $p_i = p_i(t)$  только одного элемента  $i$  от нуля до единицы включительно. Все элементы монотонных систем могут иметь только положительные или нулевые значения характеристик их значимости. Величина  $B_i^+$  положительного вклада (5) равна абсолютному изменению надежности  $P_{F/AC}(t)$  АСУТП, которое произойдет, если собственную характеристику  $p_i = p_i(t)$  надежности одного элемента  $i$  увеличить от ее текущего значения  $p_i = p_i(t)$  до единицы. Величина  $B_i^-$  отрицательного вклада (6) равна абсолютному изменению надежности  $P_F(t)$  АСУТП, которое произойдет, если собственную характеристику надежности одного элемента  $i$  уменьшить от ее текущего значения  $p_i$  до

нуля. Показатели роли элементов позволяют выработать и обосновать проектные решения по обеспечению надежности и безопасности проектируемых АСУТП.

5. Для восстанавливаемых АСУТП расчет средней наработки  $T_{OB}$  на отказ или аварийную ситуацию и среднего времени восстановления  $T_B$  осуществляется на основе формул:

$$T_{OB} = K\Gamma_{F/AC} \left( \frac{1}{\sum_{i=1}^H \xi_i \frac{1}{T_{oi}} K\Gamma_i} \right) \quad (7)$$

$$T_B = (1 - K\Gamma_{F/AC}) \left( \frac{1}{\sum_{i=1}^H \xi_i \frac{1}{T_{oi}} K\Gamma_i} \right) \quad (8)$$

6. На основе оценок (7) и (8) определяется приближенное значение еще одной важной характеристики надежности восстанавливаемой АСУТП – вероятности  $P_{BF}(t)$  ее безотказной работы в течение заданного времени  $t$ . Расчет этого показателя основывается на гипотезе о том, что распределение протяженности суммарного времени безотказной работы и последующего времени восстановления системы близко к экспоненциальному закону и может характеризоваться эквивалентной интенсивностью

$$\lambda_{\text{э}} = \frac{1}{T_{OB} + T_B} \quad (9)$$

Тогда вероятности безотказной работы и отказа, в течение времени  $t$  функционирования восстанавливаемой АСУТП любой структуры, составят

$$P_{BF/BAC}(t) = e^{-\lambda_{\text{э}} t} = e^{-\frac{t}{T_{OB} + T_B}}; \quad Q_{BF/BAC}(t) = 1 - P_{BF/BAC}(t). \quad (10)$$

## ПРИМЕРЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ АВТОМАТИЗИРОВАННОГО СТРУКТУРНО-ЛОГИЧЕСКОГО МОДЕЛИРОВАНИЯ

### Пример 1. Автоматизированное моделирование и расчет надежности программно-логического контроллера АСУТП

#### Этап 1. Постановка задачи и построение СФЦ

Первичное описание структуры рассматриваемого в Примере 1 программно-логического контроллера (ПЛК) выполнено с помощью структурно-функциональной схемы, изображенной на рис.3.

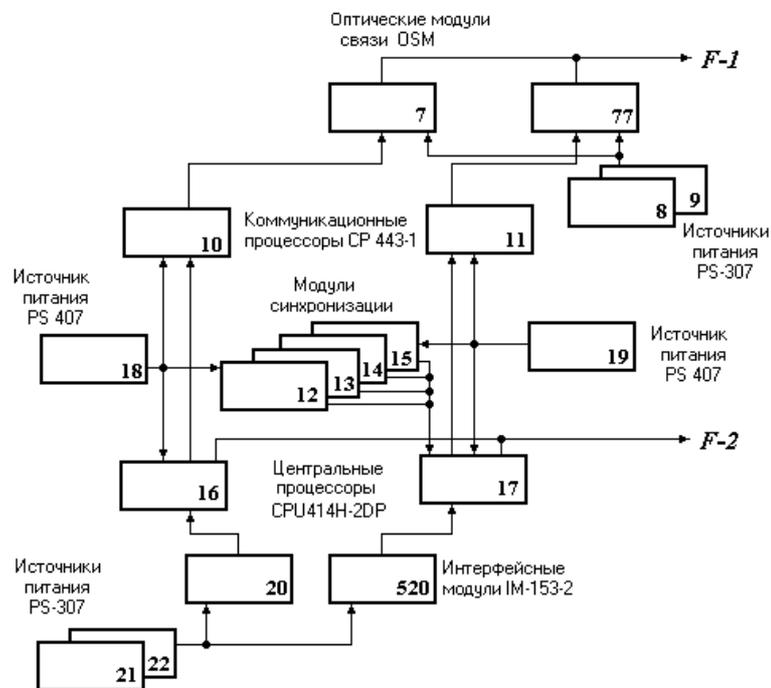


Рис.3. Функциональная схема ПЛК

В табл.1 приведен перечень всех элементов ПЛК и заданные параметры их надежности.

Параметры надежности элементов ПЛК

Таблица 1

№	Тип элемента	Обознач. на схеме	Кол-во	$T_{oi}$ (год)	$T_{vi}$ (час)
1	Интерфейсный модуль IM 153-2	20, 250	2	47.60	2
2	Центральный процессор CPU414H-2DP	16,17	2	14.70	4
3	Коммуникационный процессор CP 443-1	10,11	2	20.60	3
4	Оптический модуль связи OSM	7, 77	2	33.60	4
5	Модуль синхронизации	12,13,14,15	4	150.00	2
6	Источник питания PS 307	8,9,21,22	4	148.00	0.5
7	Источник питания PS 407	18, 19	2	71.50	0.5

Параметрами надежности элементов, заданными в табл.1, являются:  $T_{oi}$  – средняя наработка элемента до отказа в годах;  $T_{vi}$  – среднее время восстановления элемента в часах.

В дополнение к функциональной схеме, приведенной на рис.3, сформулированы описания логических условий реализации элементами ПЛК их выходных функций. Эти данные позволяют осуществить последовательное построение СФЦ ПЛК, основные этапы которого представлены на рис.4.

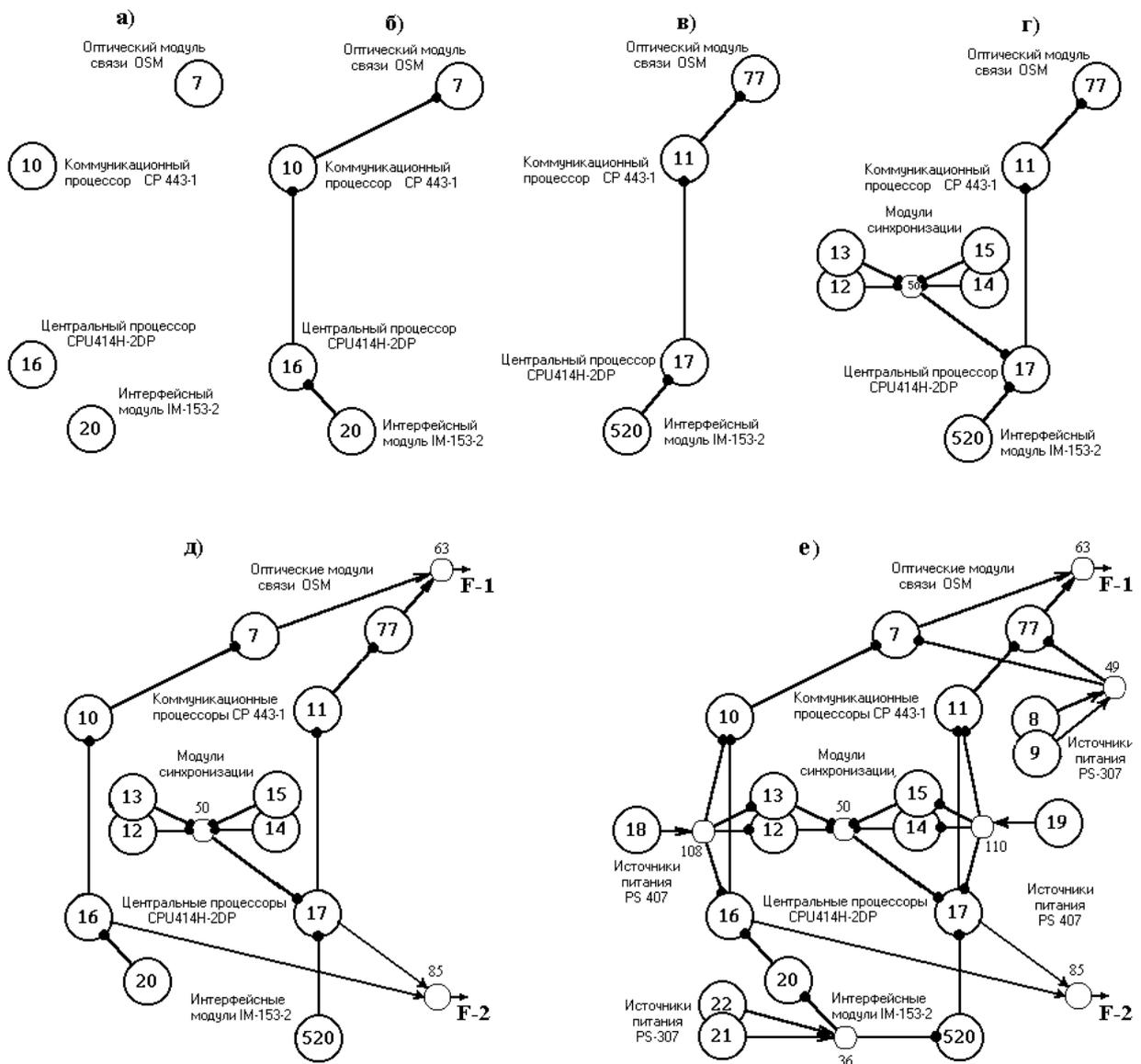


Рис.4. Этапы построения схемы функциональной целостности ПЛК

а) Основные функции контроллера реализуются с помощью четырех элементов – интерфейсного модуля 20, центрального процессора 16, коммуникационного процессора 10 и оптического модуля связи 7. На рис.4.а эти элементы представлены функциональными вершинами  $i = 20, 16, 10$  и  $7$  разрабатываемой СФЦ. Эти вершины обозначают в СФЦ события (состояния) безотказной работы  $x_{20}, x_{16}, x_{10}$  и  $x_7$  соответствующих элементов контроллера.

б) Основные элементы контроллера имеют следующие логические условия реализации выходных функций в системе. Оптический модуль связи 7 реализует свою функцию  $y_7$ , если, во-первых, сам не отказал ( $x_7$ ), и, во-вторых, если его работа обеспечивается выходной функцией  $y_{10}$  коммуникационного процессора 10. В свою очередь, функция  $y_{10}$  определяется собственной работоспособностью коммуникационного процессора  $x_{10}$ , а также выходной функцией  $y_{16}$  центрального процессора 17. Тот, в свою очередь, обеспечивается функцией  $y_{20}$  интерфейсного модуля 20. Эта последовательность функционального подчинения представлена графически в СФЦ на рис.4.б.

в) Для увеличения надежности в контроллере реализовано групповое резервирование главной последовательности элементов (см рис.4.б) резервной последовательностью (см. рис.4.в) с элементами 520, 17, 11 и 77 соответственно (см. также рис.1). Логические условия функционирования элементов резервной последовательности в системе аналогичны уже рассмотренным условиям работы основных элементов. На рис.4.в изображен фрагмент СФЦ резервной группы элементов контроллера.

г) Согласованная работа резервной группы элементов контроллера обеспечивается непрерывной безотказной работой одновременно четырех модулей синхронизации 12, 13, 14, и 17. Непосредственное обеспечение синхронизации работы резервной цепи осуществляется в контроллере через центральный процессор 17 (см. рис.3). В СФЦ условие безотказной работы одновременно всех модулей синхронизации представлено на рис.4.г с помощью четырех конъюнктивных дуг (заканчиваются точками), заходящих в фиктивную вершину с номером 50. Конъюнктивная дуга из фиктивной вершины 50 в функциональную вершину 17 представляет условие синхронизации работы резервного центрального процессора 17 и, следовательно, всей резервной цепи элементов контроллера.

д) Контроллер реализует две выходные функции. Функция  $F-1$  управления технологическими процессами реализуется при условии функционирования хотя бы одного из двух оптических модулей связи 7 (основной режим) или 77 (резервный режим). Функция

F-2 управления противоаварийной защитой реализуется при функционировании хотя бы одного из двух центральных процессоров 16 (основной режим) или 17 (резервный режим). Эти условия реализации контроллером своих функций представлены в СФЦ на рис.4.д. с помощью двух фиктивных вершин 85 и 63. Входящие в них пары дизъюнктивных дуг (заканчиваются стрелками) представляют реализованные в контроллере возможности основного и резервного режимов работы.

е) Для обеспечения гарантированного питания в ПЛК реализовано групповое и поэлементное дублирование трех независимых групп источников питания (см. рис.3 и рис.4.е):

- коммуникационные процессоры и модули синхронизации основной (16, 10, 12, 13) и резервной (17, 11, 14, 15) цепей элементов контроллера обеспечиваются отдельными источниками автономного питания 18 и 19 типа PS-407;
- интерфейсные модули 20 и 520 обеспечиваются питанием от двух дублированных источников 8 и 9 типа PS-307;
- оптические модули связи 7 и 77 обеспечиваются питанием от двух других дублированных источников 21 и 22 типа PS-307;

Сформулированные условия обеспечения питания элементов контроллера представлены в СФЦ с помощью фиктивных вершин 108, 110, 49 и 37. Заходящие в них дизъюнктивные дуги обозначают режимы нагруженного резервирования источников питания. Исходящие из этих вершин конъюнктивные дуги охватывают те элементы контроллера, которые обеспечиваются питанием от соответствующих источников.

Окончательный вариант СФЦ контроллера изображен на рис.4.е. Логическими критериями функционирования контроллера являются:

$$Y_{F-1} = y_{63} - \text{условие реализации функции } F-1 \text{ управления} \quad (11)$$

технологическими процессами;

$$Y_{F-2} = y_{85} - \text{условие реализации функции } F-2 \text{ управления} \quad (12)$$

автоматической противоаварийной защитой (ПАЗ).

*Этап 2. Применение ПК АСМ для оценки надежности и безопасности ПЛК*

### **2.1. Моделирование и расчет показателей надежности ПЛК**

После завершения подготовки исходных данных, они вводятся в ПК АСМ. На рис.5 изображено типовое окно подготовки и ввода графа СФЦ и параметров надежности элементов (см. табл.1) рассматриваемого ПЛК.

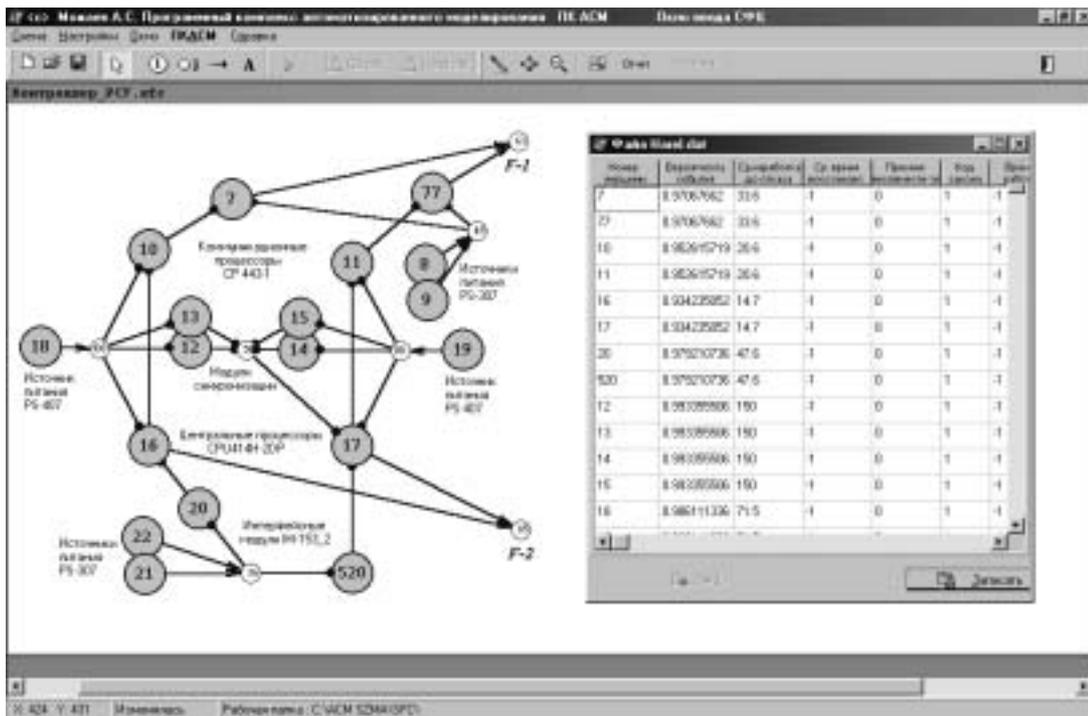


Рис.5. Окно ввода исходных данных типового ПК АСМ

После ввода в ПК АСМ графа СФЦ и параметров элементов все последующие этапы моделирования и расчетов показателей надежности выполняются автоматически. На рис.6 изображено типовое окно автоматизированного моделирования и расчетов ПК АСМ.

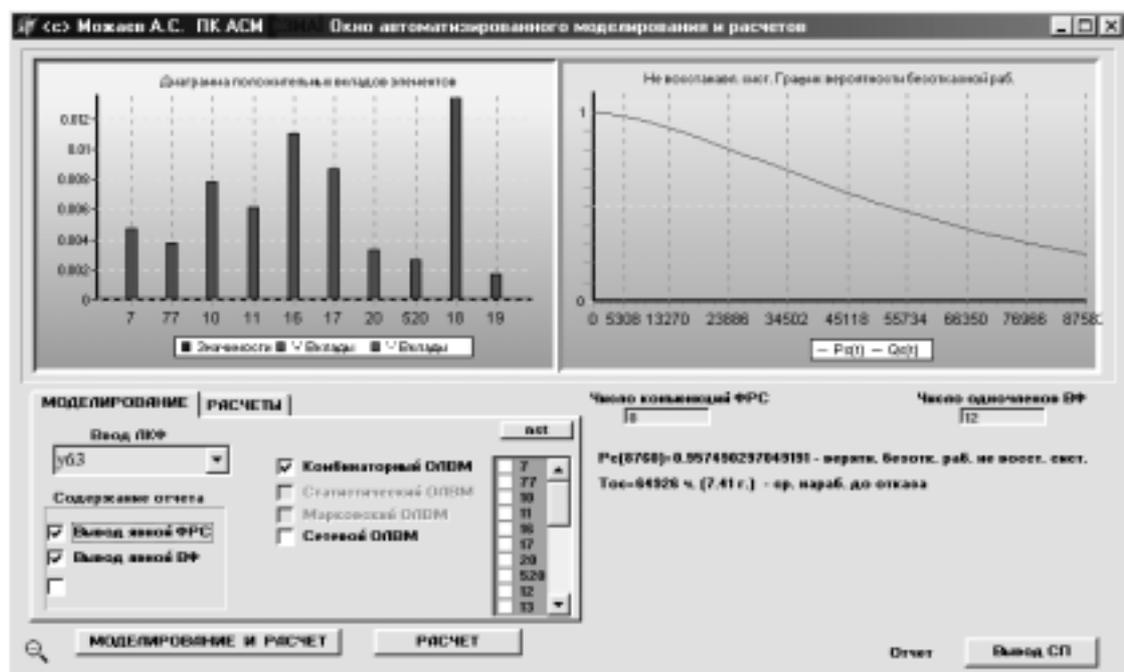


Рис.6. Окно моделирования и расчетов ПК АСМ

В окне на рис.6 приведены основные результаты моделирования надежности ПЛК по критерию (11)  $Y_{F-1} = y_{63}$  - реализации функции  $F-1$ .

Полные результаты автоматизированного моделирования и расчетов показателей надежности ПЛК составляют:

1) Логическая функция работоспособности ПЛК по  $F-I$ , которая включает 8 конъюнкций (кратчайших путей успешного функционирования)

$$\begin{aligned}
 Y_{F-1} = y_{63} = & x_7 \cdot x_{10} \cdot x_{16} \cdot x_{20} \cdot x_{18} \cdot x_8 \cdot x_{22} \vee \\
 & \vee x_7 \cdot x_{10} \cdot x_{16} \cdot x_{20} \cdot x_{18} \cdot x_9 \cdot x_{22} \vee \\
 & \vee x_7 \cdot x_{10} \cdot x_{16} \cdot x_{20} \cdot x_{18} \cdot x_8 \cdot x_{21} \vee \\
 & \vee x_7 \cdot x_{10} \cdot x_{16} \cdot x_{20} \cdot x_{18} \cdot x_9 \cdot x_{21} \vee \\
 & \vee x_{77} \cdot x_{11} \cdot x_{17} \cdot x_{520} \cdot x_{12} \cdot x_{13} \cdot x_{14} \cdot x_{15} \cdot x_{18} \cdot x_{19} \cdot x_8 \cdot x_{22} \vee \\
 & \vee x_{77} \cdot x_{11} \cdot x_{17} \cdot x_{520} \cdot x_{12} \cdot x_{13} \cdot x_{14} \cdot x_{15} \cdot x_{18} \cdot x_{19} \cdot x_9 \cdot x_{22} \vee \\
 & \vee x_{77} \cdot x_{11} \cdot x_{17} \cdot x_{520} \cdot x_{12} \cdot x_{13} \cdot x_{14} \cdot x_{15} \cdot x_{18} \cdot x_{19} \cdot x_8 \cdot x_{21} \vee \\
 & \vee x_{77} \cdot x_{11} \cdot x_{17} \cdot x_{520} \cdot x_{12} \cdot x_{13} \cdot x_{14} \cdot x_{15} \cdot x_{18} \cdot x_{19} \cdot x_9 \cdot x_{21}
 \end{aligned} \tag{13}$$

Логическая ФРС (13) получена в ПК АСМ на основе преобразования СФЦ, изображенной на рис.5, по ЛКФ (11) с помощью специального универсального графоаналитического метода, алгоритма и программы логического моделирования, разработанных в ОЛВМ.

2) Многочлен расчетной вероятностной функции безотказности управления технологическими процессами, который состоит из 12 одночленов.

$$\begin{aligned}
 P_{F-1}(t) = & p_{77} p_{11} p_{17} p_{520} p_{12} p_{13} p_{14} p_{15} p_{18} p_{19} q_8 p_9 q_{22} p_{21} + \\
 & + p_7 p_{10} p_{16} p_{20} p_{18} q_8 p_9 q_{22} p_{21} + \\
 & + p_{77} p_{11} p_{17} p_{520} p_{12} p_{13} p_{14} p_{15} p_{18} p_{19} q_8 p_9 p_{22} + \\
 & + p_{77} p_{11} p_{17} p_{520} p_{12} p_{13} p_{14} p_{15} p_{18} p_{19} p_8 q_{22} p_{21} + \\
 & + p_7 p_{10} p_{16} p_{20} p_{18} q_8 p_9 p_{22} + \\
 & + p_7 p_{10} p_{16} p_{20} p_{18} p_8 p_9 q_{22} p_{21} + \\
 & + p_{77} p_{11} p_{17} p_{520} p_{12} p_{13} p_{14} p_{15} p_{18} p_{19} p_8 p_{22} + \\
 & + p_7 p_{10} p_{16} p_{20} p_{18} p_8 p_{22} - \\
 & - p_7 p_{77} p_{10} p_{11} p_{16} p_{17} p_{20} p_{520} p_{12} p_{13} p_{14} p_{15} p_{18} p_{19} p_8 p_{22} - \\
 & - p_7 p_{77} p_{10} p_{11} p_{16} p_{17} p_{20} p_{520} p_{12} p_{13} p_{14} p_{15} p_{18} p_{19} p_8 q_{22} p_{21} - \\
 & - p_7 p_{77} p_{10} p_{11} p_{16} p_{17} p_{20} p_{520} p_{12} p_{13} p_{14} p_{15} p_{18} p_{19} q_8 p_9 p_{22} - \\
 & - p_7 p_{77} p_{10} p_{11} p_{16} p_{17} p_{20} p_{520} p_{12} p_{13} p_{14} p_{15} p_{18} p_{19} q_8 p_9 q_{22} p_{21}
 \end{aligned} \tag{14}$$

Многочлен (14) получен в ПК АСМ на основе специального комбинированного метода, алгоритма и программы преобразования ФРС (13).

3) Все параметры  $p_i = p_i(t)$ , подставляемые в многочлен (14) являются функциями времени. Значение  $t = 1 \text{ год} = 8760 \text{ час.}$  одинаковое для всех параметров и составляет заданное время работы всего ПЛК (наработку). Результаты расчетов показателей надежности

невосстанавливаемого ПЛК по функции  $F-1$  управления технологическими процессами, составляют:

$$\begin{aligned} P_{F-1}(1z) &= 0.958 - \text{вероятность безотказной работы контроллера по } F-1; \\ T_{oF-1} &= 7.41 \text{ год.} - \text{средняя наработка до отказа по } F-1; \end{aligned} \quad (15)$$

В верхней части рис.6 приведены диаграмма положительных вкладов отдельных элементов контроллера в надежности реализации функции  $F-1$  и график закона распределения времени безотказной работы.

4) Результаты расчетов показателей надежности восстанавливаемого контроллера, по функции  $F-1$  управления технологическими процессами, полученные в ПК АСМ на основе ВФ (14) с учетом среднего времени восстановления каждого элемента (см. табл.1 столбец  $T_{Bi}$ ) составили:

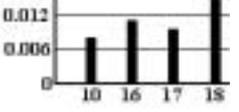
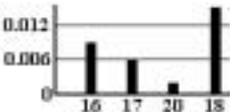
$$\begin{aligned} KГ_{F-1} &= 0.99999839 - \text{коэффициент готовности;} \\ T_{HOF-1} &= 71.37 \text{ г.} - \text{средняя наработка на отказ;} \\ T_{BF-1} &= 1 \text{ ч.} - \text{среднее время восстановления;} \\ P_{BF-1}(1z) &= 0.986. - \text{вероятность безотказной работы.} \end{aligned} \quad (16)$$

Автоматическое моделирование и расчет показателей надежности контроллера по функции  $F-2$  управления противоаварийной защитой выполняется по аналогичной методике на основе критерия (12)  $Y_{F-2} = y_{85}$ .

Общие результаты моделирования и расчета показателей надежности ПЛК по функциям  $F-1$  и  $F-2$  приведены в табл.2.

Таблица 2

Сводные результаты проектного расчета надежности ПЛК

$F$	$\frac{\Phi PC}{ВФ}$	Не восстанавливаем. ПЛК		Восстанавливаемый ПЛК			Графики положительных вкладов элементов
		$P_F(t)$	$T_{oF}$	$KГ_F$	$T_{юF}/T_{вF}$	$P_{всF}(t)$	
$F-1$	$\frac{8}{12}$	0.957	7.41 г.	0.9999984	$\frac{71.37 \text{ ч.}}{1.0 \text{ ч.}}$	0.986	
$F-2$	$\frac{4}{6}$	0.976	12.28 г.	0.9999986	$\frac{71.46 \text{ ч.}}{1.0 \text{ ч.}}$	0.986	

## 2.2. Моделирование и расчет вероятностей аварийных ситуаций ПЛК

Государственным стандартом ГОСТ 24.701-86 для обеспечения требуемого уровня безопасности АСУТП предусмотрен вероятностный анализ возможных аварийных ситуаций. Это соответствует требованиям п.2.6 РД 03-418-01 определения вероятности или частоты аварийной ситуации, и является частью оценки риска аварии. В технологии АСМ этот анализ может производиться путем вычисления вероятностей возникновения исключительных (аварийных, критических) ситуаций.

Для каждой аварийной ситуации в проектируемой АСУТП Заказчик формулирует условия ее возникновения. Эти условия описываются соответствующим логическим критерием  $Y_{AC}(\{y_i\})$ . Например, если в качестве аварийной ситуации в рассматриваемом ПЛК определен одновременный отказ первой  $F-1$  и второй  $F-2$  функций, то соответствующий логический критерий составит

$$Y_{AC} = \bar{y}_{63} \cdot \bar{y}_{85} \quad (17)$$

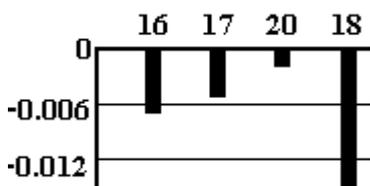
Методика вероятностного анализа безопасности АСУТП для заданной аварийной ситуации аналогична методике автоматизированного моделирования и расчета надежности. Сначала логические критерии аварийных ситуаций вводятся в ПК АСМ, затем автоматически определяются соответствующие логические ФРС, многочлены ВФ и выполняются расчеты.

Полученная с помощью ПК АСМ логическая ФРС для критерия (17) имеет вид

$$Y_{AC} = \bar{y}_{63} \cdot \bar{y}_{85} = \bar{x}_{18} \vee \bar{x}_{22}x_{21} \vee \bar{x}_{20}\bar{x}_{14} \vee \bar{x}_{20}\bar{x}_{15} \vee \bar{x}_{20}\bar{x}_{12} \vee \bar{x}_{20}\bar{x}_{13} \vee \bar{x}_{20}\bar{x}_{19} \vee \bar{x}_{20}\bar{x}_{520} \vee \bar{x}_{17}\bar{x}_{20} \vee \bar{x}_{16}\bar{x}_{14} \vee \bar{x}_{16}\bar{x}_{15} \vee \bar{x}_{16}\bar{x}_{12} \vee \bar{x}_{16}\bar{x}_{13} \vee \bar{x}_{16}\bar{x}_{19} \vee \bar{x}_{16}\bar{x}_{520} \vee \bar{x}_{16}\bar{x}_{17} \quad (18)$$

ФРС (18) представляет 16 минимальных сечений (комбинаций) отказов элементов, каждый из которых достоверно приводит к возникновению указанной аварийной ситуации.

Вероятностная функция, полученная в ПК АСМ путем преобразования ФРС (18), включает 30 одночленов. Вычисленные на ее основе нижние оценки вероятности возникновения аварийной ситуации (без учета восстановлений элементов) и наибольшие вклады элементов контроллера составляют

$$P_{AC}(t = 8760 \text{ час}) = 0.024$$


Element	Contribution
16	-0.006
17	-0.004
20	-0.002
18	-0.006

(19)

Вычисленное в ПК АСМ верхнее значение вероятности этой аварийной ситуации (с учетом восстановлений элементов) равна

$$P_{\text{вАС}}(t = 8760 \text{ час.}) = 0.014 \quad (20)$$

### 2.3. Моделирование и анализ отказоустойчивости ПЛК

Кроме вероятностной оценки возможности возникновения аварийных ситуаций для обеспечения и управления безаварийностью АСУТП часто требуется определение наиболее опасных сочетаний (комбинаций и/или последовательностей) отказов или поражений элементов, которые непосредственно приводят к возникновению аварийной ситуации. Решение указанной задачи называют анализом отказоустойчивости АСУТП.

Анализ отказоустойчивости является важной дополнительной детерминированной характеристикой надежности и безопасности АСУТП. В технологии АСМ он выполняется в два этапа:

- для множества всех выходных функций  $F$  системы задаются противоположные логические критерии их не реализации (функционального отказа) и определяются, с помощью ПК АСМ, соответствующие ФРС (множества минимальных сечений отказов);
- на основе сравнительного анализа этих множеств по всем функциям  $F$  определяют наиболее опасные сечения отказов, которые приводят к тяжелым последствиям или вызывают множественные отказы функций АСУТП. Далее эти данные могут использоваться для обоснования проектных и управленческих решений по обеспечению (повышению) надежности и безопасности АСУТП.

Пример анализа отказоустойчивости рассматриваемого ПЛК выполнен по следующим критериям отказов двух его функций:

$$\bar{Y}_{F-1} = \bar{y}_{63}; \quad \bar{Y}_{F-2} = \bar{y}_{85}. \quad (21)$$

С помощью ПК АСМ определены соответствующие минимальные сечения отказов:

$$\begin{aligned} \bar{Y}_{F-1} = \bar{y}_{63} = & \bar{x}_{18} \vee \bar{x}_{20} \bar{x}_1 \vee \bar{x}_{16} \bar{x}_{14} \vee \bar{x}_{10} \bar{x}_{14} \vee \bar{x}_7 \bar{x}_{14} \vee \bar{x}_{20} \bar{x}_{15} \vee \bar{x}_{16} \bar{x}_{15} \vee \bar{x}_{10} \bar{x}_{15} \vee \bar{x}_7 \bar{x}_{15} \vee \\ & \vee \bar{x}_{20} \bar{x}_{12} \vee \bar{x}_{16} \bar{x}_{12} \vee \bar{x}_{10} \bar{x}_{12} \vee \bar{x}_7 \bar{x}_{12} \vee \bar{x}_{20} \bar{x}_{13} \vee \bar{x}_{16} \bar{x}_{13} \vee \bar{x}_{10} \bar{x}_{13} \vee \bar{x}_7 \bar{x}_{13} \vee \\ & \vee \bar{x}_{20} \bar{x}_{19} \vee \bar{x}_{16} \bar{x}_{19} \vee \bar{x}_{10} \bar{x}_{19} \vee \bar{x}_7 \bar{x}_{19} \vee \bar{x}_{22} \bar{x}_{21} \vee \bar{x}_{20} \bar{x}_{520} \vee \bar{x}_{16} \bar{x}_{520} \vee \bar{x}_{10} \bar{x}_{520} \vee \\ & \vee \bar{x}_7 \bar{x}_{520} \vee \bar{x}_{17} \bar{x}_{20} \vee \bar{x}_{16} \bar{x}_{17} \vee \bar{x}_{10} \bar{x}_{17} \vee \bar{x}_7 \bar{x}_{17} \vee \bar{x}_{11} \bar{x}_{20} \vee \bar{x}_{11} \bar{x}_{16} \vee \bar{x}_{10} \bar{x}_{11} \vee \\ & \vee \bar{x}_7 \bar{x}_{11} \vee \bar{x}_8 \bar{x}_9 \vee \bar{x}_{77} \bar{x}_{20} \vee \bar{x}_{77} \bar{x}_{16} \vee \bar{x}_{77} \bar{x}_{10} \vee \bar{x}_7 \bar{x}_{77} \end{aligned} \quad (22)$$

$$\begin{aligned} \bar{Y}_{F-2} = \bar{y}_{85} = & \bar{x}_{18} \vee \bar{x}_{16} \bar{x}_{14} \vee \bar{x}_{20} \bar{x}_{15} \vee \bar{x}_{16} \bar{x}_{15} \vee \bar{x}_{20} \bar{x}_{12} \vee \bar{x}_{16} \bar{x}_{12} \vee \bar{x}_{16} \bar{x}_{13} \vee \bar{x}_{20} \bar{x}_{13} \vee \bar{x}_{20} \bar{x}_{19} \vee \\ & \vee \bar{x}_{16} \bar{x}_{19} \vee \bar{x}_{22} \bar{x}_{21} \vee \bar{x}_{20} \bar{x}_{520} \vee \bar{x}_{16} \bar{x}_{520} \vee \bar{x}_{17} \bar{x}_{20} \vee \bar{x}_{16} \bar{x}_{17} \vee \bar{x}_7 \bar{x}_{17} \end{aligned} \quad (23)$$

Сравнительный анализ конъюнкций (22) и (23) показывает, что к отказу одновременно двух функций контроллера приводят 16 минимальных комбинаций отказов элементов. При этом наибольшую опасность представляет элемент 18 (источник питания PS 407). Одиночный отказ (уничтожение, повреждение) только одного этого элемента нарушает работоспособность контроллера сразу по всем его функциям, т.е. вызывает возникновение аварийной ситуации (17).

Следующими по уровню опасности являются все парные отказы элементов, составляющие функцию (23). Они также приводят к отказу всех функций контроллера. Остальные сечения из (22) приводят к отказу только одной функции  $F-1$ .

### **Этап 3. Использование результатов автоматизированного моделирования для повышения надежности и безопасности ПЛК**

На основе результатов выполненного автоматизированного моделирования и расчетов (см. табл.2, (18), (19), (22) и (23)) можно заключить, что наибольшее увеличение надежности и безопасности проектируемого ПЛК, при минимальных затратах на дополнительное оборудование, можно получить путем введения в структуру системы еще одного резервного источника питания PS 407 для элемента 18. На рис.7 приведена СФЦ нового варианта структуры ПЛК с резервным блоком питания 118.

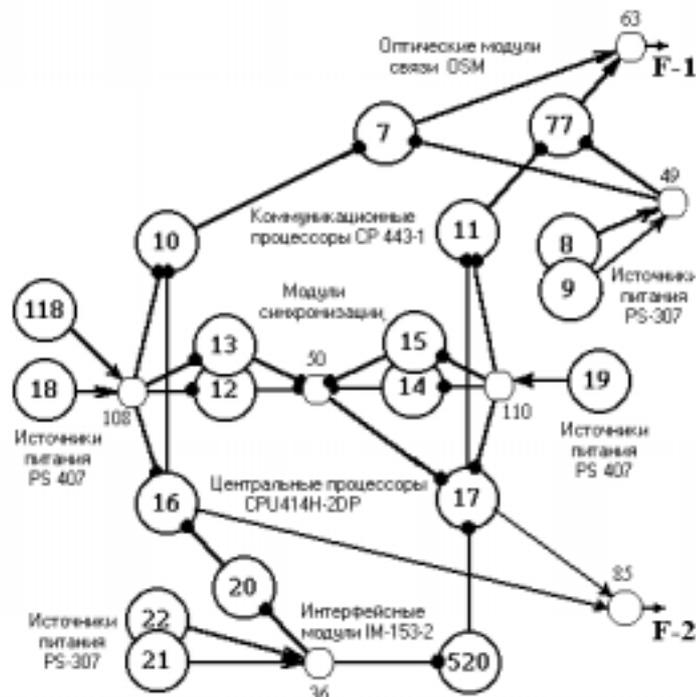
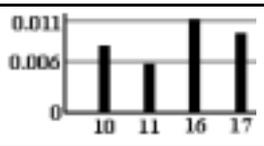
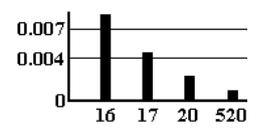
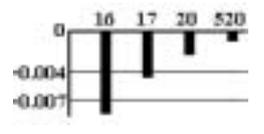


Рис.7. СФЦ ПЛК с дополнительным блоком питания 118

Общие результаты автоматизированного моделирования и расчетов показателей надежности и безопасности нового варианта ПЛК приведены в табл.3.

Таблица 3

Результаты расчета надежности нового варианта ПЛК

$F$	$\frac{\Phi PC}{B\Phi}$	Не восстановл. ПЛК		Восстанавливаемый ПЛК			Графики положительных вкладов элементов
		$P_F(t)$	$T_{oF}$	$KГ_F$	$T_{ноF}/T_{вF}$	$P_{всF}(t)$	
F-1	$\frac{16}{24}$	<b>0.971</b>	<b>7.98 г.</b>	<b>0.9999999954</b>	$\frac{38243 \text{ з.}}{1.63 \text{ ч.}}$	<b>0.999974</b>	
F-2	$\frac{8}{12}$	<b>0.976</b>	<b>12.28 г.</b>	<b>0.9999999984</b>	$\frac{116523 \text{ з.}}{1.60 \text{ ч.}}$	<b>0.9999914</b>	
АС	$\frac{8}{16}$	<b><math>P_{AC}(t)=0.011</math></b>		<b><math>P_{вас}(t)=0.0000086</math></b>			

Сравнение этих результатов с данными, приведенными в табл.2, и формулах (19) и (20) показывают, что добавление элемента 118 привело к существенному увеличению надежности и безопасности проектируемого ПЛК.

**Пример 2. Автоматизированное моделирование и расчет безопасности заправочной операции**

На рис.8 изображено "дерево отказа" заправочной операции, приведенное в РД 03-418-01 "Методические указания по проведению анализа риска опасных производственных объектов" Госгортехнадзора России. Смысловое содержание и вероятности свершения исходных событий, заданные в РД 03-418-01, указаны в табл.4

Вершинами заданного дерева представлены исходные события  $i = 1, 2, \dots, 13$  сценария возможных вариантов возникновения аварийной ситуации в ходе выполнения заправочной операции. Комбинации событий 1-6 определяют условия отказа подсистемы автоматической противоаварийной защиты, событий 7-11 – ошибки оператора, события 12, 13 – отказ технических средств аварийного отключения насоса.

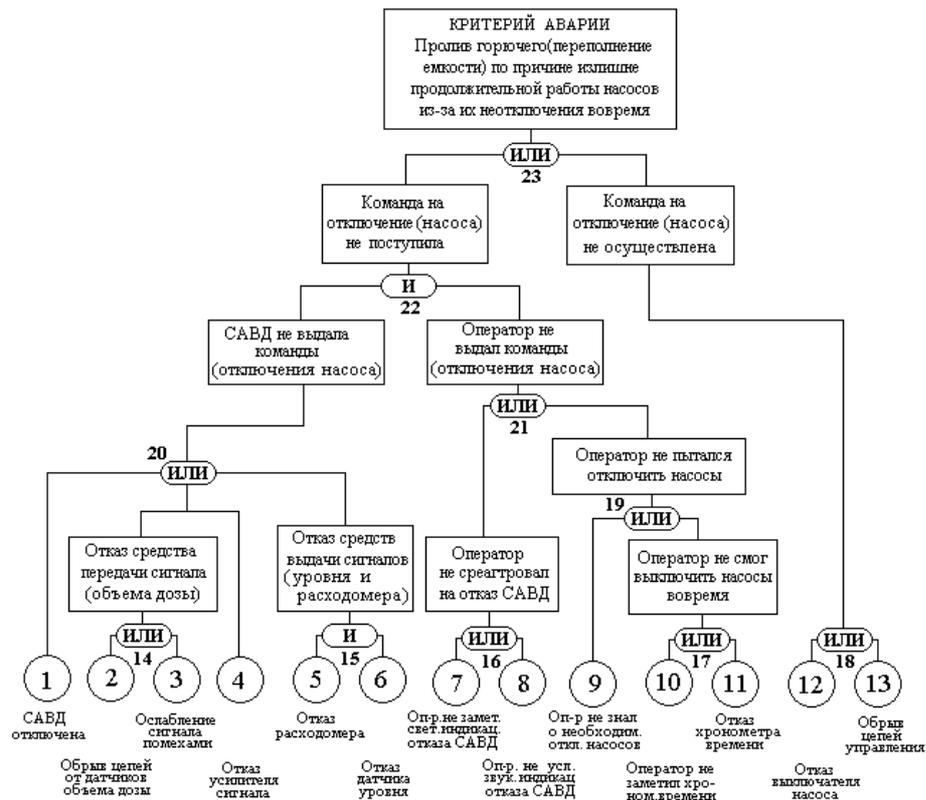


Рис.8. "Дерево отказа" заправочной операции

Таблица 4

№ <i>i</i>	Исходные события "дерева отказа" заправочной операции	Вероятн. $P_i$
1	Система автоматической выдачи дозы (САВД) оказалась отключенной	0,0005
2	Обрыв цепей передачи сигнала от датчиков объема дозы	0,00001
3	Ослабление сигнала выдачи дозы помехами	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	0,005
8	Оператор не услышал звуковой сигнализации об отказе САВД	0,001
9	Оператор не знал о необходимости отключения насоса по истечении заданного времени	0,001
10	Оператор не заметил индикации хронометра об истечении заданного 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 данном примере рассматривается методика применения технологии и программного комплекса автоматизированного структурно-логического моделирования для вероятностного и детерминированного анализа безопасности автоматизированной системы управления заправочной операцией на опасном производственном объекте.

На рис.9 изображен вариант СФЦ тождественный дереву отказов, приведенному на рис.8.

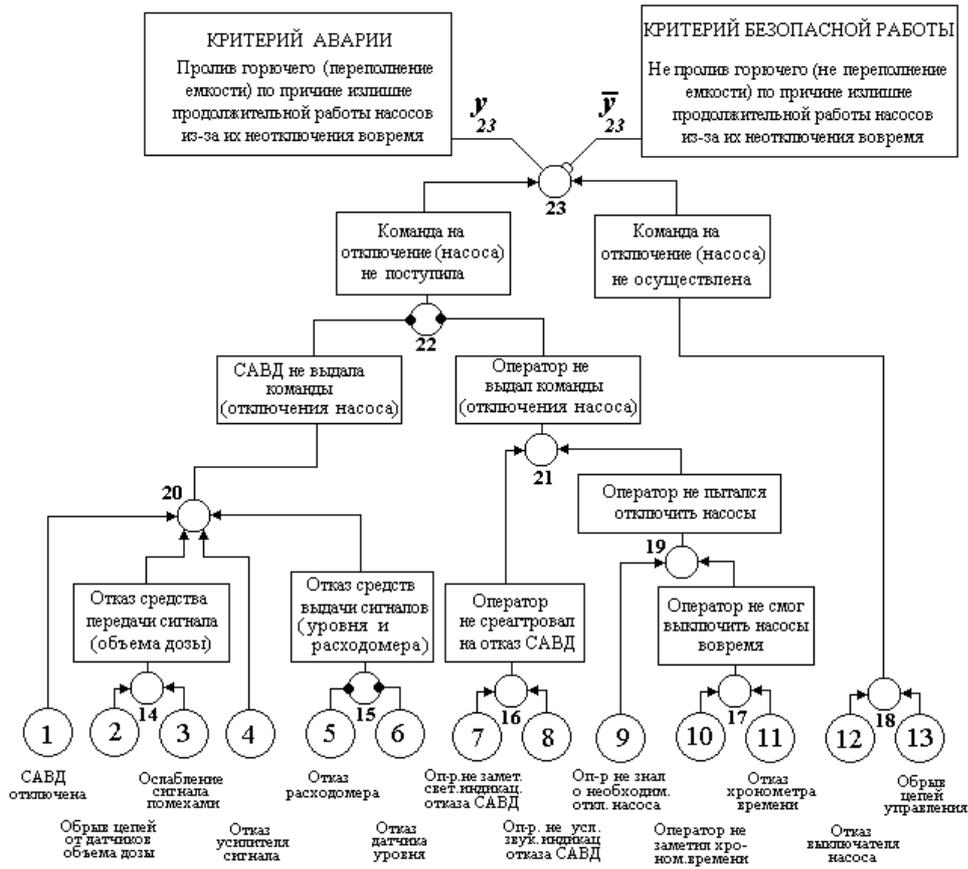


Рис.9. СФЦ заправочной операции

СФЦ на рис.9 подобна дереву отказов, приведенному на рис.8. Внешние отличия заключаются только в том, что логические связки "И" и "ИЛИ" дерева отказов (на рис.8 отмечены номерами 14-23) заменены в СФЦ на рис.9 фиктивными вершинами, с соответствующими конъюнктивными и дизъюнктивными заходящими дугами.

Универсальность аппарата СФЦ позволяет (в отличие от дерева отказов) использовать два выхода фиктивной вершины 23 – прямой  $y_{23}$  и инверсный  $\bar{y}_{23}$ . При этом, прямой выход  $y_{23}$  на рис.9 (как и верхнее событие в дереве отказов на рис.8) является критерием возникновения аварии ( $Y_{AC} = y_{23}$ ), а инверсный выход  $\bar{y}_{23}$  – критерием противоположного функционального события – безаварийного (безопасного) выполнения заправочной операции ( $Y_{безопасности} = \bar{y}_{23}$ ).

Полученные с помощью ПК АСМ логические ФРС составляют:

$$\begin{aligned}
 Y_{AC} = y_{23} = & x_1 \cdot x_7 \vee x_2 \cdot x_7 \vee x_3 \cdot x_7 \vee x_4 \cdot x_7 \vee x_5 \cdot x_6 \cdot x_7 \vee x_1 \cdot x_8 \vee x_2 \cdot x_8 \vee \\
 & \vee x_3 \cdot x_8 \vee x_4 \cdot x_8 \vee x_5 \cdot x_6 \cdot x_8 \vee x_1 \cdot x_9 \vee x_2 \cdot x_9 \vee x_3 \cdot x_9 \vee x_4 \cdot x_9 \vee \\
 & \vee x_5 \cdot x_6 \cdot x_9 \vee x_1 \cdot x_{10} \vee x_2 \cdot x_{10} \vee x_3 \cdot x_{10} \vee x_4 \cdot x_{10} \vee x_5 \cdot x_6 \cdot x_{10} \vee \\
 & \vee x_1 \cdot x_{11} \vee x_2 \cdot x_{11} \vee x_3 \cdot x_{11} \vee x_4 \cdot x_{11} \vee x_5 \cdot x_6 \cdot x_{11} \vee x_{12} \vee x_{13}
 \end{aligned} \quad (24)$$

$$\begin{aligned}
 Y_{\text{безопасности}} = \bar{y}_{23} = & \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3 \cdot \bar{x}_4 \cdot \bar{x}_5 \cdot \bar{x}_{12} \cdot \bar{x}_{13} \vee \\
 & \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3 \cdot \bar{x}_4 \cdot \bar{x}_6 \cdot \bar{x}_{12} \cdot \bar{x}_{13} \vee \\
 & \vee \bar{x}_7 \cdot \bar{x}_8 \cdot \bar{x}_9 \cdot \bar{x}_{10} \cdot \bar{x}_{11} \cdot \bar{x}_{12} \cdot \bar{x}_{13}
 \end{aligned} \quad (25)$$

ФРС (24) включает в себя 27 минимальных пропускных сочетаний, а ФРС (25) – три минимальных отсечных сочетаний, которые точно совпадают с результатами, приведенными в РД 03-418-01.

С помощью ПК АСМ определены многочлены ВФ и выполнены расчеты вероятностей возникновения аварии (технический риск) и безаварийного выполнения заправочной операции:

$$\begin{aligned}
 P_{AC} = & p1 p7 q12 q13 + q1 p2 p7 q12 q13 + q1 q2 p3 p7 q12 q13 + q1 q2 q3 p4 p7 q12 q13 + \\
 & + q1 q2 q3 q4 p5 p6 p7 q12 q13 + p1 q7 p8 q12 q13 + q1 p2 q7 p8 q12 q13 + q1 q2 p3 q7 p8 q12 q13 + \\
 & + q1 q2 q3 p4 q7 p8 q12 q13 + q1 q2 q3 q4 p5 p6 q7 p8 q12 q13 + p1 q7 q8 p9 q12 q13 + \\
 & + q1 p2 q7 q8 p9 q12 q13 + q1 q2 p3 q7 q8 p9 q12 q13 + q1 q2 q3 p4 q7 q8 p9 q12 q13 + \\
 & + q1 q2 q3 q4 p5 p6 q7 q8 p9 q12 q13 + p1 q7 q8 q9 p10 q12 q13 + q1 p2 q7 q8 q9 p10 q12 q13 + \\
 & + q1 q2 p3 q7 q8 q9 p10 q12 q13 + q1 q2 q3 p4 q7 q8 q9 p10 q12 q13 + \\
 & + q1 q2 q3 q4 p5 p6 q7 q8 q9 p10 q12 q13 + p1 q7 q8 q9 q10 p11 q12 q13 + \\
 & + q1 p2 q7 q8 q9 q10 p11 q12 q13 + q1 q2 p3 q7 q8 q9 q10 p11 q12 q13 + \\
 & + q1 q2 q3 p4 q7 q8 q9 q10 p11 q12 q13 + q1 q2 q3 q4 p5 p6 q7 q8 q9 q10 p11 q12 q13 + \\
 & + p12 + q12 p13 = \underline{0.000029}
 \end{aligned} \quad (26)$$

$$\begin{aligned}
 P_{\text{безопасности}} = & q1 q2 q3 q4 q5 p6 q12 q13 + q7 q8 q9 q10 q11 q12 q13 + \\
 & + q1 q2 q3 q4 q6 q12 q13 - q1 q2 q3 q4 q6 q7 q8 q9 q10 q11 q12 q13 - \\
 & - q1 q2 q3 q4 q5 p6 q7 q8 q9 q10 q11 q12 q13 = \underline{0.999971}
 \end{aligned} \quad (27)$$

На рис.10 приведена диаграмма вкладов показателей надежности отдельных элементов в безопасность выполнения заправочной операции, полученная с помощью ПК АСМ.

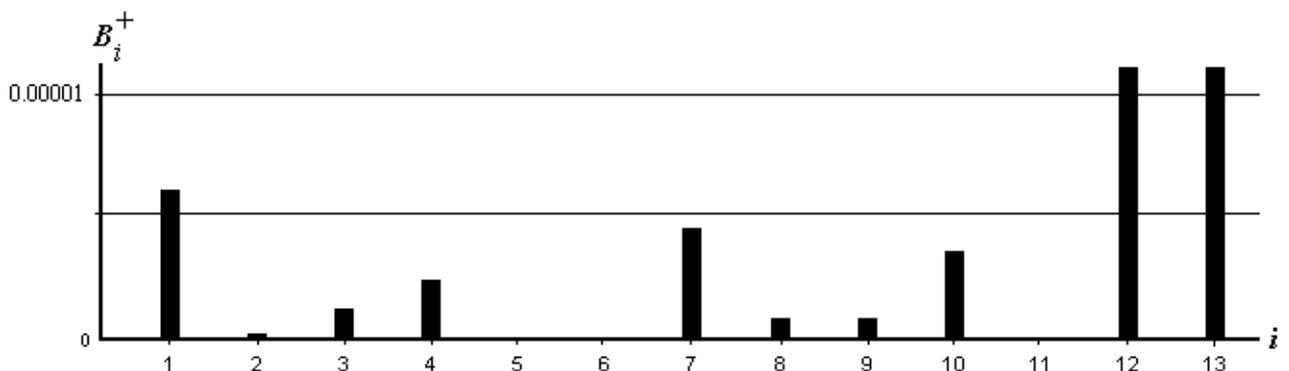


Рис.10. Диаграмма вкладов элементов в безопасность выполнения заправочной операции