Министерство науки и образования Украины
Харьковский национальный университет имени В.Н. Каразина
Факультет компьютерных наук

Андреев Ф.М., Бердников А.Г.

# Методические рекомендации по проектной оценке надежности

Харьков
2016

УДК (665.6/.7:681.5). 002.2

ББК 35.514:32.965

Ф 33

Утверждено на заседании кафедры теоретической и прикладной системотехники Харьковского национального университета имени В.Н. Каразина Протокол № ____ от 2016 года

## Аннотация

Методические рекомендации по проектной оценке надежности содержат методику анализа надежности автоматизированной системы управления технологическим процессом (АСУ ТП). В качестве примера, рассмотрена система управления газокомпрессорного цеха магистрального газопровода. Эти методические рекомендации могут быть использованы при выполнении практических занятий по учебным дисциплинам «Основы теории эксплуатации сложных радиоэлектронных систем», «Проектирование компьютеризированных систем управления», а также при выполнении дипломных и курсовых работ.

## Анотація

Методичні рекомендації щодо проектної оцінки надійності містять методику аналізу надійності автоматизованої системи управління технологічним процесом (АСУ ТП). Як приклад, розглянуто систему управління газокомпресорного цеху магістрального газопроводу. Ці методичні рекомендації можуть бути використані при виконанні практичних занять з навчальних дисциплін «Основи теорії експлуатації складних радіоелектронних систем», «Проектування комп'ютеризованих систем управління», а також при виконанні дипломних і курсових робіт.

## Annotation

Methodical recommendations about project reliability estimation contain a methodology of analyzing the reliability of the automated process control system (APCS). As an example, consider the control system of gas compressor plant gas trunkline. These methodical recommendations can be used in the case of practical training execution on subjects "A basis of the theory of difficult radio-electronic systems operation", "Design of the computerized management systems", and also in the case of degree and term papers execution.

**Ключевые слова**

Показатели надежности АСУ, структурная схема расчета надежности, методика анализа надежности АСУ ТП на этапе проектирования, классы безопасности АСУ ТП, уровни интегральной надежности.

**Ключові слова**

Показники надійності АСУ, структурна схема розрахунку надійності, методика аналізу надійності АСУ ТП на етапі проектування, класи безпеки АСУ ТП, рівні інтегральної надійності.

**Keywords**

Reliability of APCS indexes, flow diagram of reliability calculation, methodology of analyzing the reliability APCS on the stage of the planning, safety classes of APCS, integral reliability levels.

## Содержание

**Введение**

Оценка показателей надежности АСУ производится в соответствии с ГОСТ 24.701-86 «Надежность автоматизированных систем управления» по следующим показателям:

надежность реализации функций системы;

опасность возникновения в системе аварийных ситуаций.

Для первого показателя описание надежности осуществляется по:

единичным показателям надежности;

комплексным показателям надежности.

В качестве комплексных показателей безотказности и ремонтопригодности в ГОСТ 24.701-86 используются:

1. Коэффициент готовности системы к выполнению i-й функции – ($K_Г$);
2. Коэффициент технического использования системы – ($K_{ТИ}$);
3. Коэффициент сохранения эффективности системы.

В целом по набору показателей надежности ГОСТ 24.701-86 на порядок превосходит стандарты Международной электротехнической комиссии (МЭК) IEC 61 508.

Недостаток ГОСТ 24.701-86 состоит в отсутствии конкретных методик расчета этих показателей перечисленных показателей и практических примеров их применения.

## 1. Выбор метода анализа надежности для АСУ ТП

Практически все производители оборудования разного рода систем для нахождения базовых значений интенсивности отказов отдельных компонентов, узлов, модулей используют рекомендации справочника МО США Military Handbook: «Realibility Prediction of Electronic Egnipment», MCL-HDBK-217F, 2 December 1991.

К настоящему времени фактически это справочное руководство стало стандартом для производителей электронного оборудования всех отраслей промышленности Запада.

Для оценки интегрального уровня надежности (безопасности) абсолютное большинство поставщиков и разработчиков систем на Западе опираются на технический отчет безопасного технического допуска DTR 84.02–ISATR 84.0.02 (Оборудование безопасности систем – техника оценки интегрального уровня безопасности), разработанный подкомиссией ISATR 84.02.

Этот отчет рекомендует 3 методики анализа надежности (безопасности) систем, которые дают ответ на вопрос: будет ли система в состоянии выполнить возложенные на нее функции, а именно:

1. Метод логических блок-диаграмм;

2. Анализ дерева отказов;

3. Марковский анализ.

Первый этап для всех указанных методик одинаков. Он предполагает получение исходной информации для расчета интенсивности отказов по каждому элементу, модулю, блоку или комплектной подсистемы.

Марковский анализ на практике используется очень редко из-за сложности систем дифференциальных уравнений, которые имеют место при анализе реальных систем.

Метод анализа дерева отказов идеально подходит для анализа видов, последствий и критичности отказов (ГОСТ 27.310-95), но особенно для технической диагностики, т.е. поиска отказавшего элемента системы. Иногда этот метод используется при проектировании новых систем или устройств.

Некоторые эксперты рассматривают его как компромисс между простотой метода логических блок-диаграмм (блок–схем) и полнотой марковского анализа для вычисления уровня надежности.

Поэтому далее рассмотрим метод, основанный на традиционном анализе логических блок-схем надежности (безопасности), который обеспечивает первое приближение для оценки требуемого уровня надежности.

## 2. Основные допущения

**2.1.** Структурная схема для расчета надежности любой из подсистем, входящих в сложную радиоэлектронную систему, рассматривается как сочетание последовательно и параллельно связанных элементов.

Последовательное соединение относится к подсистемам или элементам сложных систем, работающим без резерва.

Надежность системы $P_s(t)$, состоящей из $n$ последовательных элементов, характеризуемая вероятностью безотказной работы, согласно теории вероятностей равна

$$P^{ПС}_s(t) = \prod_{i=1}^{n} P_i(t) , \qquad (1)$$

где $P_i(t)$ – вероятность безотказной работы i-го элемента.

Если известна интенсивность каждого элемента $\lambda_i$ , то надежность системы равна

$$P_s(t) = e^{-\sum \lambda i\, t} . \qquad (2)$$

Параллельное соединение относится к резервированным подсистемам или элементам. Блок-схема параллельного соединения приведена на Рис.1.

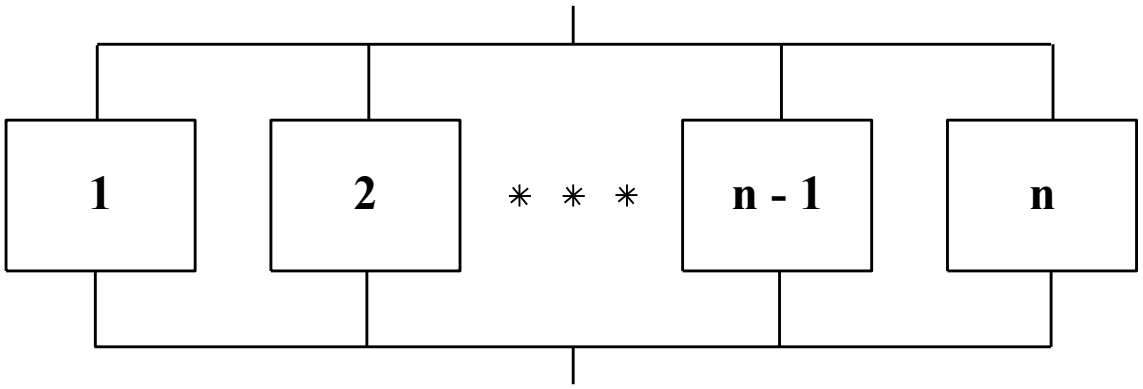


Рис.1. Блок-схема параллельного соединения

Вероятность отказа $P_s(t)$ для такой системы в соответствии с теорией вероятностей равна

$$P_s(t) = \prod_{i=1}^{n} [1 - P_i(t)], \qquad (3)$$

А вероятность безотказной работы (надежность) равна

$$P^{ПР}_s(t) = 1 - \prod_{i=1}^{n} [1 - P_i(t)], \qquad (4)$$

Если все элементы идентичны, т.е. $\lambda_i = \lambda = const$, то

$$P_s(t) = [1 - P_i(t)]^n \quad \text{и} \quad P^{ПР}_s(t) = 1 - [1 - e^{-\lambda t}]^n, \qquad (5)$$

**2.2.** Оценка надежности делается при следующих предположениях:

существующая система контроля сложной системы является идеальной, т.е. отсутствуют ошибки 1-го рода (ложные тревоги) и 2-го рода (необнаружения отказов).

система восстановления также является идеальной, т.е. нет ограничений по количеству одновременно восстанавливаемых единиц аппаратуры.

**2.3.** Рассматривается абстрактная сумма всех интенсивностей отказов $\lambda_i$ по всем устройствам. При этом понятие критического отказа не используется, т.е. все единичные отказы считаются критическими.

**2.4.** Среднее время наработки на отказ – ***MTBF*** (согласно стандарту IEC 61 508) или $T_{oi}$ (согласно ГОСТ 24.701-86) определяется в соответствии с [ 1 ] как

$$MTBF = T_{Oi} = 1 / \lambda_i \quad . \qquad (6)$$

**2.5.** Среднее время на восстановление ***MTBR*** (согласно стандарту IEC 61 508) или $T_{Bi}$ (согласно ГОСТ 24.701-86) [ 1 ]

$$MTBR = T_{Bi} = 1 / \mu_i \quad , \qquad (7)$$

где $\mu_i$ – интенсивность восстановления.

**2.6.** Готовность – вероятность для системы (подсистемы, компонента, устройства) быть работоспособной (готовой) в определенный момент времени характеризуется коэффициентом готовности [ 1 ]

$$K_{Гi} = T_{Oi} / (T_{Oi} + T_{Bi}) = \mu_i / (\lambda_i + \mu_i) \qquad (8)$$

**2.7.** В случае последовательного соединения $n$ элементов результирующая интенсивность отказов $\lambda_s$ будет равна $\lambda_s = \sum_{i=1}^{n} \lambda_i$ , (9)

а результирующий коэффициент готовности – $K_Г = \prod_{i=1}^{n} K_{Гi}$ (10)

**2.8.** Интенсивность отказов параллельного соединения двух однотипных элементов равна $\lambda$ **.**

Для одинаковых элементов дублированной системы показатели надежности равны [2] :

$$\lambda^{1/1} \approx 2\cdot\lambda^2/\mu \qquad (11)$$

$$K_Г^{Д} \approx 1- \gamma^2 \ , \qquad (12)$$

где $\gamma = \lambda/\mu$ .

Вывод формул для расчета показателей надежности резервируемой аппаратуры с восстановлением приведен в Приложении к настоящим Рекомендациям.

**2.9.** Общее соотношение для интенсивности отказов при «скользящем» резервировании элементов [2, см. Приложение]

$$\lambda^{n/k} \approx (N -n)\cdot\lambda\cdot C_N^n\cdot\gamma^n \ , \qquad (13)$$

$$K_Г^{n/k} \approx 1- C_N^{n+1}\cdot\gamma^{n+1} \ , \qquad (14)$$

где $k$ – число рабочих элементов; $n$ – число резервных элементов;

$N = n + k$ .

Для расчета числа сочетаний используется формула [3, с.163]

$$C^{n-m}_n = C^m_n = n! / m!\cdot(n-m)! \qquad (15)$$

**2.10.** Среднее время восстановления элементов системы (подсистем) предполагается одинаковым и равным $T_В = 8$ *часов* [2, с.724].

## 3. Методика анализа надежности АСУ ТП на этапе проектирования

**Первый этап** – в общем случае АСУ ТП включает в свой состав распределенную систему управления (РСУ), систему противоаварийной защиты (ПАЗ) и систему бесперебойного электропитания (БЭП). Поэтому интенсивность отказов АСУ ТП равна

$$\lambda_{АСУ\ ТП} = \lambda_{РСУ} + \lambda_{ПАЗ} + \lambda_{БЭП} \ , \qquad (16)$$

а результирующий коэффициент готовности (надежности) [2, с. 717]

$$K_I^{АСУ\ ТП} = K_I^{РСУ} \cdot K_I^{ПАЗ} \cdot K_I^{БЭП}, \quad (17)$$

**Второй этап** – декомпозиция каждой из указанных систем (РСУ, ПАЗ, БЭП). На этом этапе в соответствии со структурными схемами составляются логические блок-схемы указанных систем.

На рис.2 приведена логическая блок-схема расчета надежности для системы БЭП [2, с. 739]

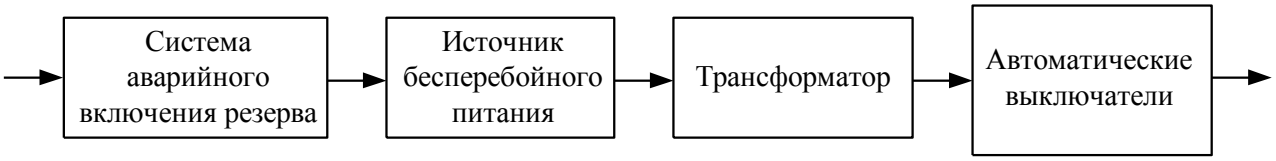


Рис.2. Однолинейная блок-схема системы БЭП

На рис.3 приведена логическая блок-схема расчета надежности для системы ПАЗ с архитектурой 2003 [2, с. 737].

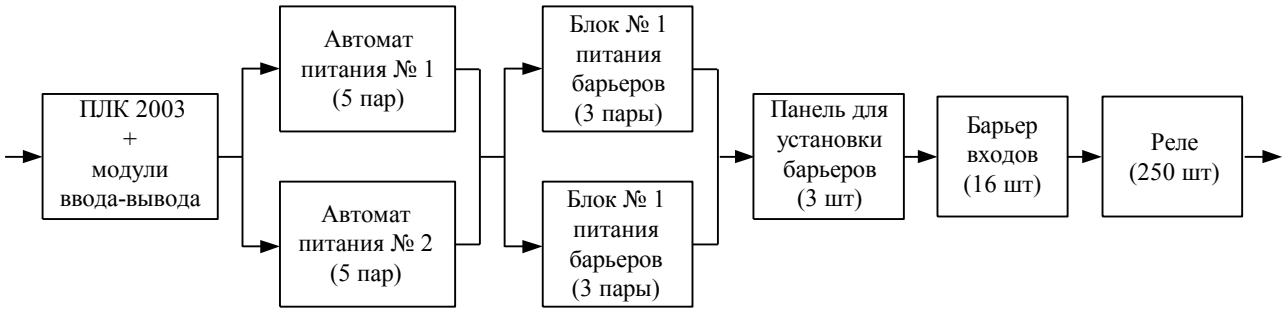


Рис. 3. Логическая блок-схема системы управления ПАЗ

Все системы управления строятся по иерархическому принципу и АСУ ТП не является исключением.

Как правило, РСУ АСУ ТП имеет один уровень. Это значит, что помимо центрального органа управления (станции технолога-оператора) на данном уровне имеется еще $M$ элементов (полевых станций управления участками), обеспечивающих управление элементами данного уровня по горизонтали. Поэтому логическая блок- схема РСУ, представленная на рис. 4, имеет вид [2, с. 718].


Рис.4. Однолинейная блок-схема распределенной системы управления АСУ ТП

**Третий этап** – декомпозиция станций технолога-оператора и станций управления участками.

Станция технолога-оператора состоит из ***m*** операторских станций. Логическая блок-схема надежности операторской станции включает в свой состав ключевые компоненты, изображенные на рис 5.

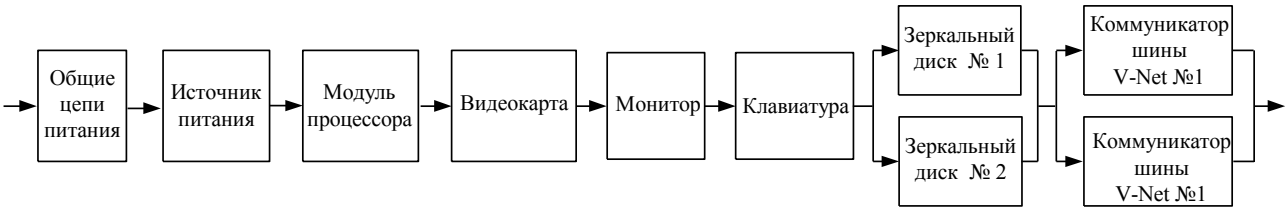


Рис. 5. Логическая блок-схема операторской станции

Станция управления участками включает в себя автомат питания, дублированный блок процессоров ПЛК для управления участком, линейку шин дистанционного ввода-вывода (шину RIO), включающих корзины для модулей ввода-вывода и дублированные коммуникационной карты шины (ККШ). На рисунке 6 изображена логическая блок-схема для расчета надежности одной станции управления участком.

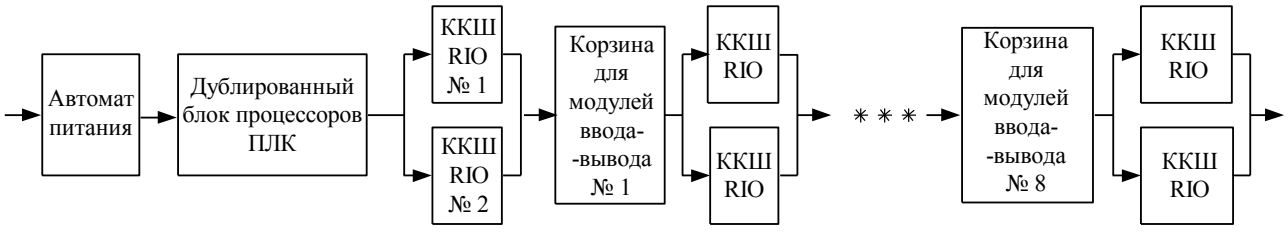


Рис. 6. Логическая блок-схема станции управления участком

**Четвертый этап** – детализация логических блок-схем для станции технолога оператора и каждой из ***S*** станций управления участками (от ***1*** до ***S*)**.

В структуре станций технолога-оператора может использоваться дублирование (троирование и т.д.) подсистемы в виде операторской станции, изображенной на рис.5

Для конфигурации станции технолога-оператора (СТО) в виде дублирующих друг друга операторных станций имеем интенсивность отказов, равную

$$\lambda_{СТО} = 2\cdot\lambda^2_{ОС}\cdot T_В, \qquad (18)$$

а коэффициент готовности –

$$K_Г^{СТО} = [\sum_{i=0}^{1} C^{2-i}{}_2\cdot(K_Г^{ОС})^{2-i}{}_{ОС}\cdot(1-K_Г^{ОС})^i] = [2\cdot K_Г^{ОС} - (K_Г^{ОС})^2] , \qquad (19)$$

где $\lambda_{ОС}$ – интенсивность отказов операторской станции;

$K_Г^{ОС}$ – коэффициент готовности операторской станции.

В случае троирования операторных станций имеем, согласно (13) и (14)

$$\lambda_{СТО} = (3 - 1 + 1)\cdot C^{3-1+1}{}_3\cdot\lambda^{3-1+1}{}_{ОС}\cdot T^2_В = 2\cdot\lambda^3_{ОС}\cdot T^2_В ; \qquad (20)$$

$$K_Г^{СТО} = \sum_{i=0}^{2} C^{3-i}{}_3\cdot(K_Г^{ОС})^{3-i}\cdot(1-K_Г^{ОС})^i = [3\cdot(K_Г^{ОС}) - 3\cdot(K_Г^{ОС})^2 + (K_Г^{ОС})^3] \qquad (21)$$

Структура станции управления каким-либо участком зависит от числа рабочих комплектов аппаратуры на этом участке.

Если число рабочих комплектов аппаратуры не менее двух, то, как правило, для обеспечения бесперебойности технологического процесса используется их «скользящее» резервирование, как более эффективное по критерию «эффективность-стоимость».

Покажем это.

Пусть подсистема состоит из двух рабочих комплектов, имеющих одинаковые интенсивности отказов.

Интенсивность отказов такой системы равна $\lambda_{раб} = 2\cdot\lambda$.

В случае использования дублирования для повышения надежности рассматриваемой системы результирующая интенсивность отказов с учетом (11) будет равна

$$\lambda_{дубл} = 2\cdot\lambda^2_{раб} = 8\cdot\lambda^2 \qquad (22).$$

В случае использования «скользящего» резервирования с учетом (13) имеем

$$\lambda_{скольз} = (4 - 2 + 1)\cdot C^3{}_4\cdot\lambda^{4-2+1} = 3\cdot[4!/(4-1)!]\cdot\lambda^3 = 12\cdot\lambda^3 \qquad (23).$$

При одинаковом количестве комплексов в рассматриваемой подсистеме (например, равном четырем), результирующая интенсивность отказов при

«скользящем» резервировании в $[12\cdot\lambda^3 / 8\cdot\lambda^2] = (3/2)\cdot\lambda$ раз меньше, т.е. среднее время наработки на отказ возрастает в $2/3\cdot\lambda$ раз.

В случае использования «скользящего» резервирования в какой-либо станции управления участком выражения для определения интенсивности отказов и коэффициента готовности определятся по формулам (11) и (12).

**5. Пятый этап** – установление интенсивностей отказов операторной станции $\lambda_{ос}$ и станции управления участком $\lambda_{уч}$ с использованием логических блок-схем, изображенных на рис. 5 и 6.

В работе [2, с.734] проведен расчет надежности станции управления участками, результаты которого представлены в таблице 1

Таблица 1

| Наименование оборудования | Интенсивность отказов (1/час) | Среднее время наработки на отказ (час) | Коэффициент готовности |
|---|---|---|---|
| Станция управления участком | $1{,}4\cdot10^{-4}$ | 7140 | 0,99888 |

Установленное значение $\lambda_{ос}$ позволяет, в свою очередь, используя результаты расчета интенсивности отказов РСУ [2, с.736], определить ориентировочные значения надежности операторной станции, которые приведены в таблице 2.

Таблица 2.

| Наименование оборудования | Интенсивность отказов (1/час) | Среднее время наработки на отказ (час) | Коэффициент готовности |
|---|---|---|---|
| Операторная станция | $5\cdot10^{-4}$ | 2000 | 0,996 |

**6. Шестой этап** – расчет показателей надежности РСУ с использованием данных, полученных на четвертом и пятом этапах.

**7. Седьмой этап** – расчет показателей надежности систем ПАЗ и БЭП с использованием логических блок-схем, изображенных на рис. 2 и 3.

Результаты расчета показателей надежности системы ПАЗ, проведенные в [2, с. 738], представлены в таблице 3.

Таблица 3.

| № п/п | Наименование показателя надежности | Значение показателя надежности |
|---|---|---|
| 1 | Интенсивность отказов (1/час) | $1{,}66 \cdot 10^{-4}$ |
| 2 | Среднее время наработки на отказ (час) | 6000 |
| 3 | Коэффициент готовности системы | 0,998666 |

Результаты расчета показателей надежности системы БЭП, проведенного в [2, с. 740], представлены в таблице 4.

Таблица 4.

| № п/п | Наименование показателя надежности | Значение показателя надежности |
|---|---|---|
| 1 | Интенсивность отказов (1/час) | $22 \cdot 10^{-6}$ |
| 2 | Среднее время наработки на отказ (час) | 45 000 |
| 3 | Коэффициент готовности системы | 0,999822 |

**8. Восьмой этап** – расчет показателей надежности АСУ ТП. На данном этапе используются результаты, полученные на шестом и седьмом этапах, которые подставляются в формулы (18, 19, 20, 21).

**9. Девятый этап** – полученное на 8-м этапе значение интегрального коэффициента готовности $K_Г^{АСУТП}$ сопоставляется с опорными значениями, характеризующими класс надежности (безопасности) АСУ ТП.

Классы надежности (безопасности) АСУ ТП приведены в стандарте МЭК IEC 61508 – «Функциональная безопасность электрических, электронных и программируемых электронных систем, связанных с безопасностью». Этот международный стандарт, разработан для определения систем безопасности (Safety Related Systen – SRS) общего вида, утвержден в 2000 году (может использоваться для любых отраслей промышленности).

Стандарт определяет четыре уровня интегральной надежности (безопасности) (**Safety Integry Level – SIL**) в зависимости от конкретной вероятности отказа выполнения требуемой функции (**Probability of Failury on Demand – PFD**). Согласно стандарту такими уровнями являются:

4-й – защита от общей катастрофы;

3-й – защита обслуживающего персонала и населения;

2-й – защита оборудования и продукции, защита от травматизма;

1-й – защита оборудования и продукции.

В таблице 5 приведены значения интегрального уровня надежности (безопасности) SIL.

Таблица 5.

| SIL | Допустимая вероятность опасного отказа ***PFD*** | Требуемый коэффициент готовности ***(1-PFD)*** | Частота опасных отказов $\lambda_{oo}$ (1/час) | Фактор снижения риска (годы) $(T = 1/\lambda_{oo})$ |
|---|---|---|---|---|
| 1 | От $10^{-2}$ до $10^{-1}$ | 90% – 99% | От $10^{-6}$ до $10^{-5}$ | От 10 лет до 100 лет |
| 2 | От $10^{-3}$ до $10^{-2}$ | 99% – 99,9% | От $10^{-7}$ до $10^{-6}$ | От 100 до 1000 лет |
| 3 | От $10^{-4}$ до $10^{-3}$ | 99,9% – 99,99% | От $10^{-8}$ до $10^{-7}$ | От 1000 до 10000 лет |
| 4 | Менее $10^{-4}$ | Более 99,99% | Менее $10^{-8}$ | Более 10000 лет |

Из таблицы 5 можно сделать следующие выводы.

Принятие уровня SIL-1 означает, что уровень опасности процесса и ограничения на экономические потери при отказе системы защиты незначительны настолько, что системе разрешается иметь 10% отказов от выполнения ею функций (или ее защиты).

Уровень надежности в 90% означает, что в случае наполнения емкости водой в одном случае из десяти может произойти ее переполнение.

Аналогично, увеличение фактора снижения риска до 100 лет при классе допуска SIL-2 не означает, что система способна проработать без опасных отказов 100 лет. Данный фактор в соответствии с ГОСТ 24.701-86 означает, что из 100 одновременно работающих систем в одной системе в течение одного года будет опасный отказ.

Порядок задания класса (уровня) допуска следующий.

Допуск основывается на требуемой величине снижения риска, которая определяется в ходе анализа опасности технологического процесса.

Диаграмма риска и классы (уровни) допуска в соответствии со стандартом IEC 61508 представлены на рис. 7.

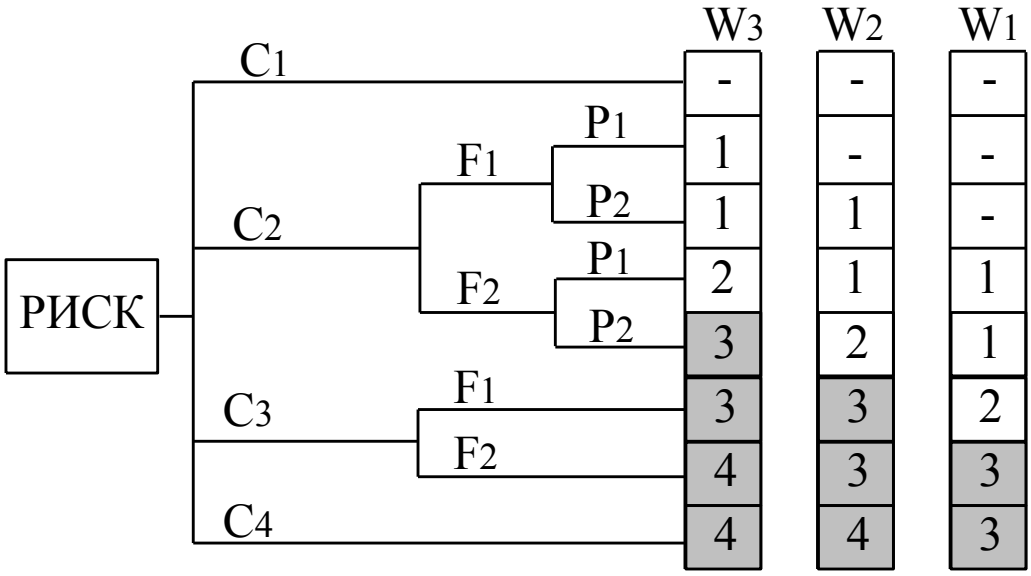


Рис. 7. Диаграмма рисков в соответствии со стандартом IEC 61 508

На рисунке 7 приняты следующие обозначения:

1. Последствия аварии: $C_1$ – незначительные травмы; $C_2$ – серьезные травмы одного или нескольких человек, смерть одного человека; $C_3$ – смерть нескольких человек; $C_4$ – катастрофические последствия, большие человеческие жертвы.

2. Частота и время нахождения в опасной зоне: $F_1$ – от редкого до относительно частого; $F_2$ – частое или постоянное.

3. Возможность избежать опасности: $P_1$ – возможно при определенных обстоятельствах; $P_2$ – невозможно.

4. Вероятность нежелательного события: $W_1$ – крайне низкая; $W_2$ – низкая; $W_3$ – высокая.

Из анализа рис. 7 следует, что взрывоопасные объекты нефтегазодобывающей, химической, нефтехимической и нефтегазоперерабатывающей промышленности должны соответствовать четвертому или третьему интегральному уровням.

В заключение следует отметить, что методика, основанная на указанных выше предположениях и заключающаяся в расчете показателей интегральной надежности, за рубежом используется фирмой Iokogawa [2, с. 708]:

## 4. Пример применения методики

Применение методики рассмотрим на примере расчета интегральной надежности (безопасности) газокомпрессорного цеха магистрального газопровода.

Упрощенная структурная схема системы управления газокомпрессорного цеха (ГКЦ) изображена на рис. 8.

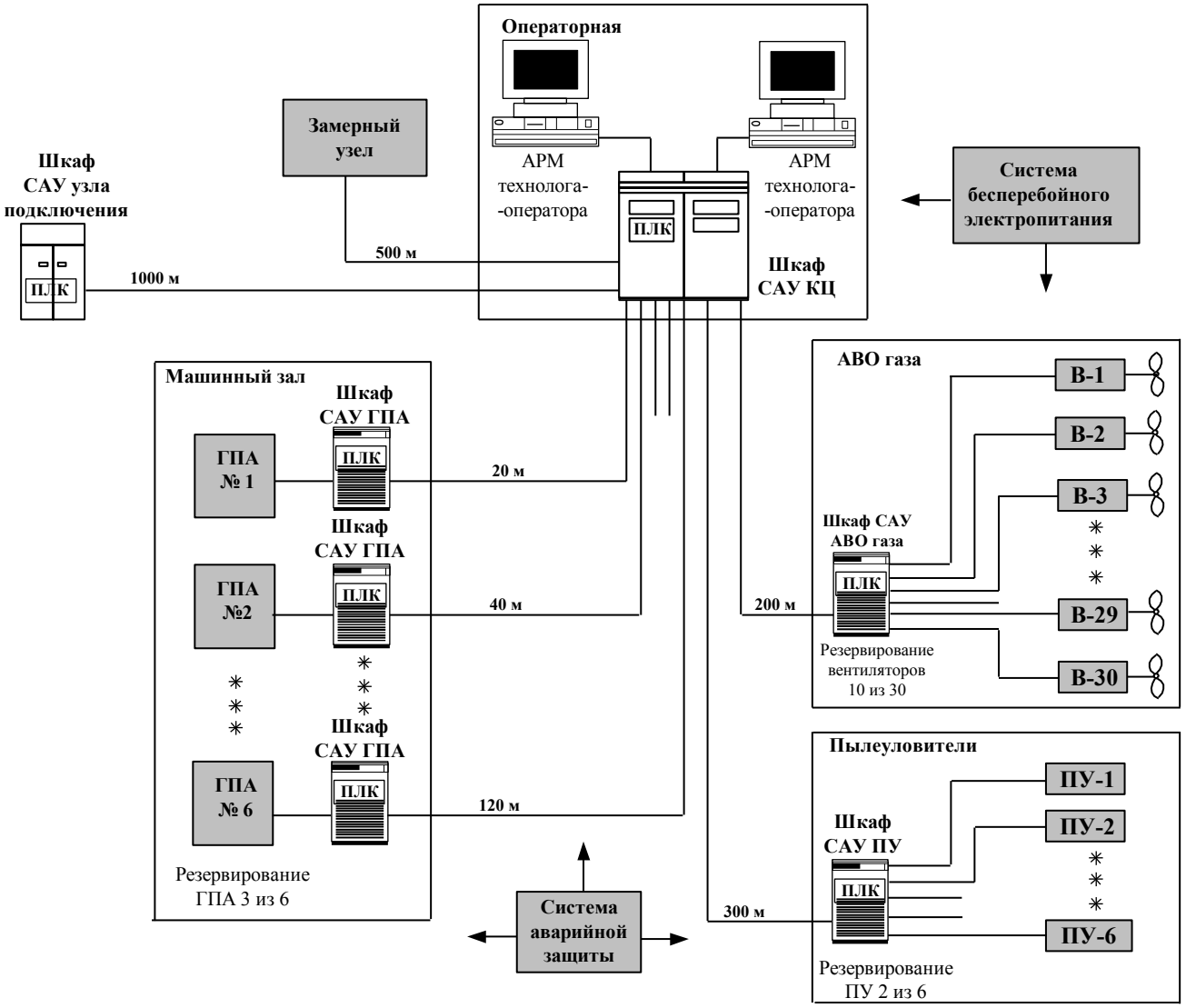


**Рис. 8. Упрощенная структурная схема системы управления газокомпрессорным цехом**

В ГКЦ компонентами технологической линии прохождения газа являются узел подключения цеха (УП) к магистральному газопроводу; участок пылеулавливателей (ПУ), очищающих транспортируемый газ; машинный зал с газоперекачивающими агрегатами (ГПА), обеспечивающими повышение давления газа в газопроводе; участок аппаратов воздушного охлаждения (АВО) газа, обеспечивающих снижение температуры газа после прохождения ГПА. Структура технологической линии ГКЦ приведена на рис. 9.

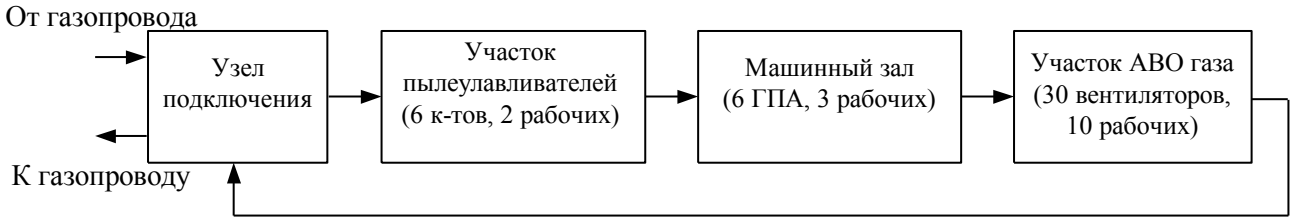


Рис. 9. Однолинейная схема технологической линии газокомпрессорного цеха

Согласно рис.8 и рис. 9 логическая блок-схема распределенной системы управления (РСУ) имеет вид, приведенный на рис.10 (САУ – система автоматического управления).


Рис. 10. Логическая блок-схема распределенной системы управления ГКЦ

Применительно к рис.10 интенсивность отказов распределенной системы управления равна

$$\lambda_{РСУ} = 2\cdot\lambda^2_{ос}\cdot T_в + \lambda^{уп}_{уч} + \lambda^{пу}_{уч} + 3\cdot C^3_6\cdot\lambda_{уч}\cdot\gamma^3 + \lambda^{аво}_{уч} =$$

$$= 4\cdot10^{-6} + 1{,}4\cdot10^{-4} + 4{,}72\cdot10^{-11} + 1{,}4\cdot10^{-4} \approx 4{,}2\cdot10^{-4}\ [1/час] \quad (24)$$

$$K_Г^{3/3} \approx 1 - C^3_6\cdot\gamma^4 \approx 1 - 15\cdot(\lambda^4_{уч} / \mu^4) \approx 1 - 15\cdot1{,}57\cdot10^{-12} \approx 1 - 2{,}4\cdot10^{-11} \approx 1 \quad (25)$$

$$[\gamma = (1{,}4\cdot10\text{-}4) / (0{,}125) = 1{,}4/0{,}125 = 11{,}2;$$

$$\gamma^4 = (11{,}2)^4\cdot10^{-16} = 15735{,}2\cdot10^{-16} = 15\cdot1{,}57\cdot10^{-12} = 23{,}6\cdot10^{-12} = 2{,}3\cdot10^{-11}]$$

$$K_Г^{РСУ} = (1-\gamma^2)\cdot K_{Гуч}^{УП}\cdot K_{Гуч}^{ПУ}\cdot K_Г^{3/3}\cdot K_{Гуч}^{АВО} \approx 0{,}99999875\cdot0{,}99888\cdot0{,}99888\cdot1\cdot0{,}99888 \approx$$

$$\approx 0{,}9966 \quad (26)$$

В таблице 6 приведены результаты расчета показателей надежности распределенной системы управления ГКЦ.

Таблица 6.

| Показатель надежности | Значение показателя |
|---|---|
| Интенсивность отказов | $\lambda_{РСУ} = 4{,}2\cdot10^{-4}$ [1/час] |
| Среднее время наработки на отказ | $T_О = 2381$ [час] |
| Коэффициент готовности РСУ | $K_Г^{РСУ} = 0{,}9966425$ |

С учетом результатов расчета надежности систем противоаварийной защиты (ПАЗ) и бесперебойного электропитания (БЭП), приведенные в таблицах 3 и 4, в таблице 7 приведены результаты проектной оценки надежности АСУ ТП газокомпрессорного цеха.

Таблица 7

| Компонента ГКЦ | Интенсивность отказов $\lambda$ [1/час] | Среднее время наработки на отказ $To = 1/\lambda$ [час] | Коэффициент готовности РСУ $K_Г^{РСУ}$ [%] |
|---|---|---|---|
| Распределенная система управления (РСУ) | $4{,}2\cdot10^{-4}$ | 2381 | 99,66 |
| Система (ПАЗ) | $1{,}66\cdot10^{-4}$ | 6000 | 99,87 |
| Система (БЭП) | $0{,}22\cdot10^{-4}$ | 45000 | 99,98 |
| АСУ ТП в целом | $6{,}08\cdot10^{-4}$ | 1645 | 99,51 |

Сопоставляя результаты расчета коэффициента готовности АСУ ТП в целом с опорными (интегральными) уравнениями (классами) SIL табл. 5, видим, что проектируемая АСУ ТП соответствует уровню SIL-2, а требуется, как минимум, SIL-3. Причинами являются недостаточный $K_Г$, прежде всего, РСУ, и, во вторую очередь, системы управления ПАЗ.

Рассмотрим вариант 1 модернизированной РСУ, который предполагает дублирование одной (любой) из трех систем управления участком.

В случае дублирования интенсивность отказов системы управления участком будет равна

$$\lambda^{дубл}_{уч} = 2\cdot\lambda^2_{уч}\cdot T_В = 3{,}92\cdot10^{-8}[1/час].$$

Тогда $\lambda_{РСУ}$ уменьшится до величины

$$\lambda^I_{РСУ} = 4\cdot10^{-6} + 3{,}92\cdot10^{-8} + 1{,}4\cdot10^{-4} + 1{,}18\cdot10^{-11} + 1{,}4\cdot10^{-4} \approx 2{,}8\cdot10^{-4}\ [1/час]\ .$$

В табл. 8 приведены результаты проектной оценки надежности АСУ ТП ГКЦ для варианта 1.

Таблица 8

| Компонента ГКЦ | Интенсивность отказов $\lambda$ [1/час] | Среднее время наработки на отказ $To = 1/\lambda$ [час] | Коэффициент готовности $K_Г$ [%] |
|---|---|---|---|
| Распределенная система управления | $\lambda_{РСУ} = 2{,}8 \cdot 10^{-4}$ | $T_{О\,РСУ} = 3571$ | $K_I^{РСУ} = 99{,}7745$ |
| Система (ПАЗ) | $\lambda_{ПАЗ} = 1{,}66 \cdot 10^{-4}$ | $T_{О\,ПАЗ} = 6000$ | $K_I^{ПАЗ} = 99{,}87$ |
| Система (БЭП) | $\lambda_{БЭП} = 0{,}22 \cdot 10^{-4}$ | $T_{О\,БЭП} = 45000$ | $K_I^{БЭП} = 99{,}98$ |
| АСУ ТП в целом | $\lambda_{АСУ} = \lambda_{РСУ} + \lambda_{ПАЗ} + \lambda_{БЭП} = 4{,}08 \cdot 10^{-4}$ | $T_{О\,АСУ} = 2137$ | $K_I^{АСУ} = K_I^{РСУ} \cdot K_I^{ПАЗ} \cdot K_I^{БЭП} = 99{,}77$ |

Значение коэффициента готовности РСУ для варианта 1 АСУ ТП, равное 99,62%, также соответствует уровню SIL-2. Выход состоит в дублировании всех трех систем управления участками.

Для варианта 2 АСУ ТП имеем

$$\lambda^{II}_{РСУ} = 4 \cdot 10^{-6} + 3{,}92 \cdot 10^{-8} + 3{,}92 \cdot 10^{-8} + 4{,}72 \cdot 10^{-11} + 3{,}92 \cdot 10^{-8} \approx 4 \cdot 10^{-6} + 4 \cdot 10^{-7} \approx 4{,}4 \cdot 10^{-6}\ [1/час];$$

$$T^{II}_{О\,РСУ} = 227000\ [час];$$

$$(K_I^{РСУ})^{II} = (1 - \gamma^2_{ОС}) \cdot (1 - \gamma^2_{уч})^3 \cdot K_I^{3/3} = 0{,}999984 \cdot (0{,}99999875)^3 \cdot 1 = 0{,}99998.$$

Следовательно, чтобы обеспечить уровень надежности $0{,}99998$ необходимо иметь систему ПАЗ с

$$K_I^{ПАЗ} = K_Г^{ТР} / K_I^{БЭП} \cdot K_I^{РСУ} = 0{,}999 / 0{,}9998 \cdot 0{,}99998 \geq 0{,}9992.$$

**Вывод.** Система ПАЗ, изображенная на рис. 3 и выпускаемая одной из зарубежных фирм, не может использоваться в АСУ ТП, в которых существует опасность взрыва.

В таких АСУ ТП необходимо использовать системы ПАЗ, у которых коэффициент готовности ПАЗ больше 99,9 % $(K_I^{ПАЗ} > 0{,}999)$.

В системе ПАЗ, изображенной на рис. 3, контроллер построен по архитектуре 2003 и является высоконадежным устройством со следующими показателями [2, с. 737]:

интенсивность отказов – $\lambda_{2003} = 7 \cdot 10^{-6}$ *1/час*;

среднее время наработки на отказ – $T_О = 140\,000$ *час*;

коэффициент готовности – $K_I^{2003} = 0{,}999943$.

Необходимая для работы в АСУ ТП с уровнем надежности SIL-3 система ПАЗ может быть получена в результате дублирования в системе ПАЗ (изображенной на рис. 3) панели для установки барьеров и барьера аналоговых входов (см. рис. 11). В этом случае может быть обеспечен необходимый коэффициент готовности $K_Г^{ПАЗ} \geq 0{,}9992$.

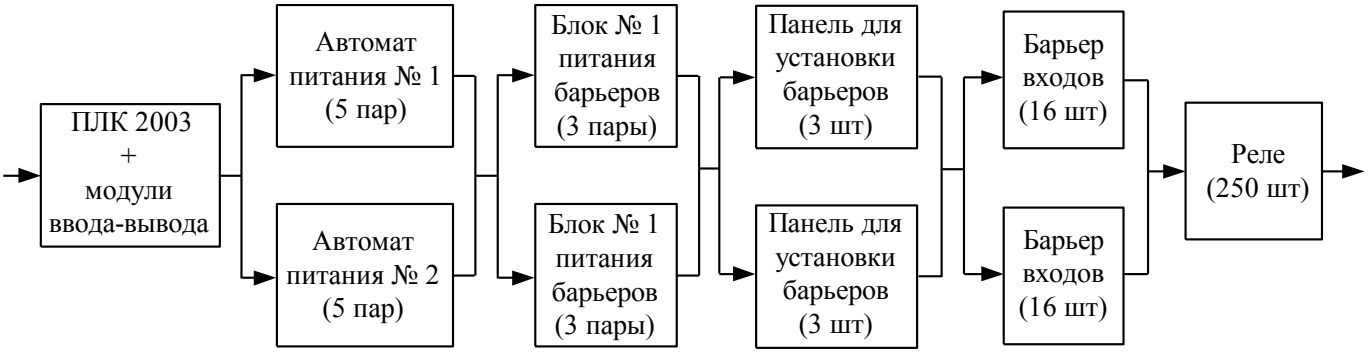


Рис. 11. Логическая блок-схема системы управления ПАЗ для работы в АСУ ТП

В примере предложен один из возможных вариантов построения АСУ ТП на базе реальных подсистем и элементов, широко используемых в современной технике.

Дальнейшее проектирование может заключаться расчете других возможных вариантов и выборе оптимального варианта по критерию «эффективность ($K_Г^{РСУ}$) – стоимость».

**Литература**

1. Андреев Ф.М. «Основи теорії єксплуатації радіоелектроних систем» /Ф.М. Андрєєв, О.Д. Єльчанінов. – Х.: ХНУ імені В.Н. Каразіна, 2014. – 281 с.

2. Федоров Ю.Н. Справочник інженера по АСУ ТП: Проектирование и разработка. Учебно-практическое пособие. / Ю.Н. Федоров – М.: Инфа – Инженерия, 2008. – 928 с.

3. Бронштейн И.Н. Справочник по математике для инженеров и учащихся ВТУЗОВ, изд. восьмое, стереотипное / И.Н. Бронштейн, К.А. Семендяев. – М.: Госиздат физико-математической литературы, 1959. –608с.

**Приложение**

## Вывод формул для расчета показателей надежности резервируемой аппаратуры с восстановлением

Среднее время наработки на отказ резервированной аппаратуры с восстановлением ($T_{ор}$) определяется выражением [ 1 ]

$$T_{ор} = \left( \sum_{i=0}^{n} Q_i / \Lambda_n \cdot Q_n \right), \qquad (1)$$

где $n$ – число резервных элементов

$$Q_0 = 1;\ Q_1 = \Lambda_0 / M_1;\ Q_2 = \Lambda_1 \cdot \Lambda_0 / M_2 \cdot M_1;\ \ldots;\ Q_i = (\Lambda_{i-1}/M_i) \cdot Q_{i-1} . \qquad (2)$$

$$\Lambda_{i-1} = k \cdot \lambda + (n - i) \cdot \lambda ; \quad M_i = i \cdot \mu , \qquad (3)$$

где $\lambda$ – интенсивность отказов;

$k$ – число рабочих элементов;

$\mu = 1/T_в$ – интенсивность восстановления;

$T_в$ – среднее время восстановления аппаратуры.

Параметр потока отказов такой системы (аппаратуры) равен

$$\lambda = 1/T_{ор} , \qquad (4)$$

а коэффициент готовности ($K_Г^{ср}$) системы с резервированием

$$K_Г^{ср} = \sum_{i=0}^{n} Q_i / \sum_{i=0}^{N} Q_i , \qquad (5)$$

где $N = n + k$ – общее число элементов системы.

Выражения (1), (4) и (5) позволяют определить показатели широко используемых на практике вариантов резервирования аппаратуры.

**Случай 1:** кратное резервирование аппаратуры $n/(k=1) = n/1$. При $n=1$ имеем вариант $1/1$ , получивший название **дублирование.**

Формула (1) для случая дублирования преобразуется к виду

$$T_{ор}^{Д} = (Q_0 + Q_1) / \Lambda_1 \cdot Q_1 . \qquad (6)$$

Так как $\Lambda_1 = 1 \cdot \lambda + (1 - 0) \cdot \lambda = 2 \cdot \lambda;$ $\Lambda_1 = \lambda ;\ M_1 = \mu ;\ M_2 = 2 \cdot \mu ;$

$$Q_0 = 1;\ Q_1 = \Lambda_0 / M_1 = 2 \cdot \lambda / M;\ Q_2 = (\Lambda_1 / M_2) \cdot (\Lambda_0 / M_1) = (\lambda / 2 \cdot M)\ (2 \cdot \lambda / M) = (\lambda / M)^2 ;$$

$$T_{ор}^{Д} = \mu / 2 \cdot \lambda^2\ (1 + 2 \cdot \lambda / \mu);\qquad \lambda_{ср}^{Д} = 2 \cdot \lambda^2 / \mu \cdot\ (1 + 2 \cdot \lambda / \mu). \qquad (7)$$

Введем параметр $\gamma = \lambda / \mu$ , характеризующий относительную интенсивность отказов элементов, тогда

$$\lambda_{ср}^{Д} = 2 \cdot \lambda \cdot \gamma / (1 + 2 \cdot \gamma) . \qquad (8)$$

Коэффициент готовности при дублировании будет равен

$$K_г^Д = (Q_0 + Q_1) / (Q_0 + Q_1 + Q_2) = 1 - \gamma^2 / (1 + 2\cdot\gamma + \gamma^2). \quad (9)$$

На практике выполняется условие $\gamma << 1$ , поэтому

$$\lambda_{ср}^Д \approx 2\cdot\lambda\cdot\gamma, \quad (10)$$

$$K_г^Д \approx 1 - \gamma^2 . \quad (11)$$

Для варианта двукратного резервирования **2/1**, когда $k = 1$; $n = 2$; $N = 3$, имеем

$$\lambda_{ср}^{троир} \approx 3\cdot\lambda\cdot\gamma^2, \quad (12)$$

$$K_г^{троир} \approx 1 - \gamma^3 . \quad (13)$$

Для варианта $n$ – кратного резервирования **n/1**, когда $k = 1$; $n = n$; $N = n + 1$, имеем

$$\lambda_{ср}^{n/1} \approx N\cdot\lambda\cdot\gamma^n , \quad (14)$$

$$K_г^{n/1} \approx 1 - \gamma^N . \quad (15)$$

**Случай 2: «скользящее резервирование»** аппаратуры **n/k**, $k>1$. В этом случае, используя формулы (1), (4) и (5), получим

$$\lambda_{ср}^{n/k} \approx (N - n)\cdot\lambda\cdot C_N^n\cdot\gamma^n , \quad (16)$$

$$K_г^{n/k} \approx 1 - C_N^{n+1}\cdot\gamma^{n+1}, \quad \text{где } N = n + k . \quad (17)$$

Приведенные формулы могут быть использованы для расчета показателей надежности компонентов разнотипных систем управления технологическими процессами.